DAP-2660

802.11ac Dual Band PoE Access Point

ユーザマニュアル

D-Link®

Building Networks for People

目次

1. お使いになるまえに 4
本製品について 5
機能概要 5
本製品の特長 5
本製品の接続モード 6
無線LANについて 7
本マニュアルについて 8
マニュアルの構成 8
マニュアルの対象者 8
表記規則 8
安全にお使いいただくために 9
無線に関するご注意 10
電波に関するご注意 10
2.4GHz 帯使用の無線機器の電波干渉に関するご注意 10
無線LAN 製品ご使用時におけるセキュリティに関するご注意 10
ご使用上の注意 11
静電気障害を防止するために 12
バッテリの取り扱いについて 12
電源の異常 12

2. 設置のしかた 13
パッケージの内容 14
動作環境 14
ネットワーク接続前の準備 14
本体各部名称 15
前面パネル 15
背面パネル 15
製品の設置 16
イーサネットケーブルの接続 16
ACアダプタの接続 16
接続例 16
マウントキットによる設置 17
アクセスポイント設置後のネットワーク接続の例 19

3. WEB GUI 画面について 20
WEB GUI画面へのログイン 21
画面の構成 22

4. Basic Settings (基本設定) 23
Basic Settings について 24
Wireless Settings（ワイヤレス設定） 24
Access Point モードを選択した場合 25
WDSモード／WDS with APモードを選択した場合 26
Wireless Clientモードを選択した場合 28
Authentication（認証）の設定について 30
LAN Settings（LAN設定） 34
IPv6 Settings（IPv6設定） 35

5. Advanced Settings (詳細設定) 36
Advanced Settings について 37
Performance Settings（パフォーマンス設定） 37
Wireless Resource Control（ワイヤレスリソースコントロール） 39
Multi-SSID Settings（マルチSSID設定） 40
VLAN Settings（VLAN設定） 41
Wireless Intrusion Protection（不正AP検知） 45
Wireless Schedule Settings（スケジュール設定） 46
Internal RADIUS Server（RADIUSサーバ） 47

ARP Spoofing Prevention Settings（ARPスプーフィング防止設定）. 48
Bandwidth Optimization（帯域幅最適化）. 49
AP Array（APアレイ）. 51
APアレイ構成図と設定手順. 51
AP Array Scan (APアレイスキャン) 52
AP Array Configuration（APアレイ設定）. 53
Auto-RF（自動RF）. 54
Load Balance（ロードバランス）. 54
Captive Portal（キャプティブポータル）. 55
Captive Portal Authentication（キャプティブポータル認証）. 55
Login Page Upload（ログイン画面アップロード）. 60
Web Redirection（Webリダイレクション）. 60
MAC Bypass Settings（MAC Bypass 設定）. 61
DHCP Server（DHCPサーバ設定）. 62
Dynamic Pool Settings（ダイナミックプール設定）. 62
Static Pool Settings（スタティックプール設定）. 63
Current IP Mapping List（IPマッピングリスト）. 64
Filters（フィルタ）. 65
Wireless MAC ACL Settings（ワイヤレスMAC ACL）. 65
WLAN Partition（WLANパーティション）. 66
Traffic Control（トラフィックコントロール）. 67
Uplink and Downlink Setting（アップリンク／ダウンリンク設定）. 67
QoS（QoS設定）. 68
Traffic Manager（トラフィックマネージャ）. 69

6. Status (ステータス) 70

Statusについて. 71
Device Information（デバイス情報）. 71
Client Information（クライアント情報）. 72
WDS Information（WDS情報）. 72
Channel Analyze（チャネル分析）. 73
Statistics（統計情報）. 74
Ethernet Traffic Statistics（イーサネットトラフィック統計情報）. 74
WLAN Traffic Statistics（WLANトラフィック統計情報）. 74
Log（ログ）. 75
View Log（ログの表示）. 75
Log Settings（ログ設定）. 76

7. 管理メニュー 78

管理メニューについて. 79
Home (ホーム画面) 79
Maintenance（メンテナンス）. 80
Administration Settings（管理者設定）. 80
Firmware Upload（ファームウェアとSSL証明書のアップロード）. 83
Configuration File Upload and Download
（コンフィグレーションファイルのアップロードとダウンロード）. 84
Time and Date Settings（時刻と日付の設定）. 85
Configuration（コンフィグレーション）. 86
設定の保存と有効化. 86
設定の破棄. 86
System（システム設定）. 87
本製品の再起動. 87
工場出荷時設定へのリセット. 87
Logout（ログアウト）. 88
Help（ヘルプ）. 88

8. 付録 89

工場出荷時設定に戻す. 90
リセットボタンで設定リセット行う. 90
Web GUIから設定リセットを行う. 90
FAQ. 91

お使いになるまえに

1

このたびは、弊社製品をお買い上げいただきありがとうございます。
本書は、製品を正しくお使いいただくための取扱説明書です。必要な場合には、いつでもご覧いただけますよう大切に保管してください。

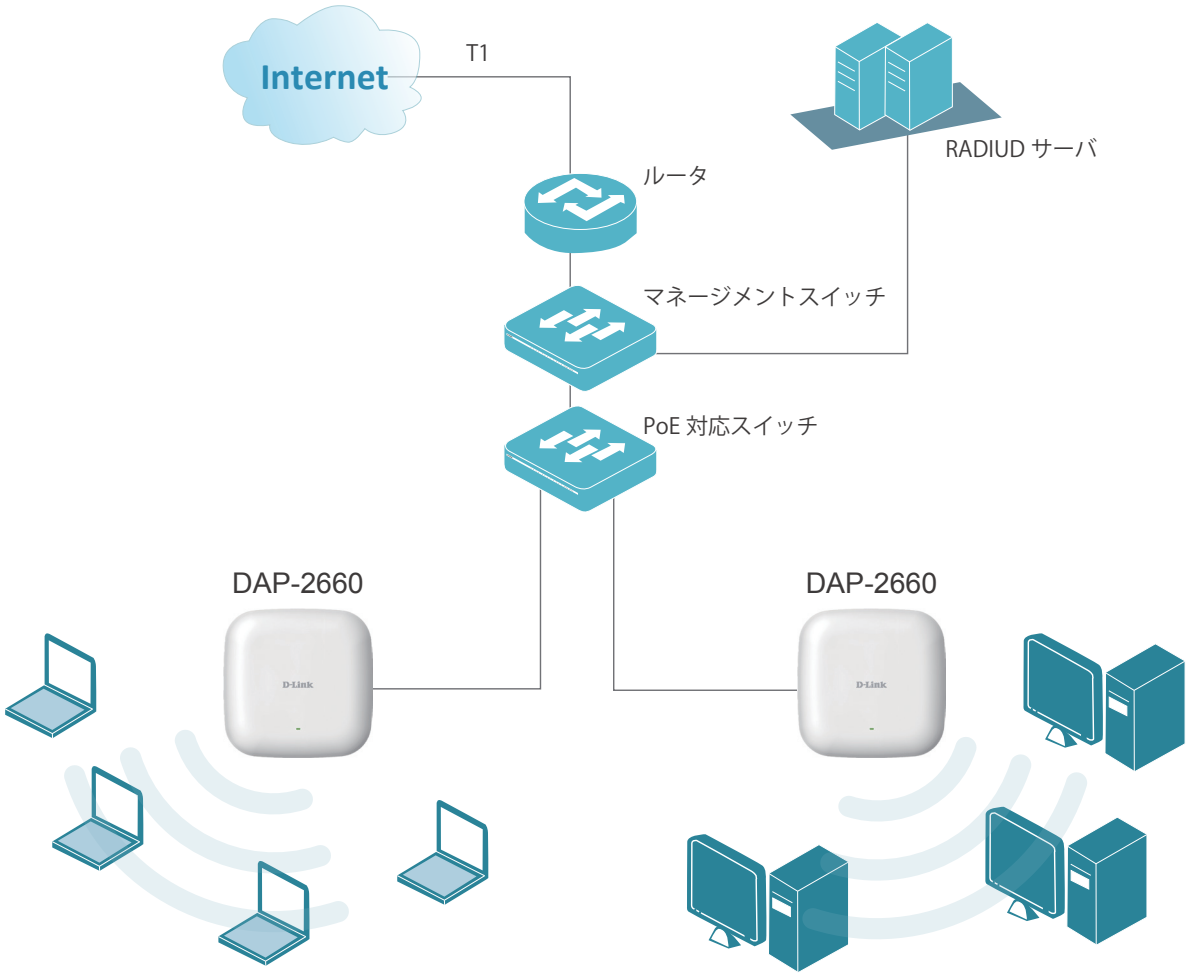
また、必ず本書および設置マニュアルをよくお読みいただき、内容をご理解いただいた上で記載事項に従ってご使用ください。

■ 本製品について……5
機能概要……5
本製品の特長……5
本製品の接続モード……6
無線LANについて……7
■ 本マニュアルについて……8
マニュアルの構成……8
マニュアルの対象者……8
表記規則……8
■ 安全にお使いいただくために……9
■ 無線に関するご注意……10
電波に関するご注意……10
2.4GHz 帯使用の無線機器の電波干渉に関するご注意……10
無線LAN 製品ご使用時におけるセキュリティに関するご注意……10
■ ご使用上の注意……11
■ 静電気障害を防止するために……12
■ バッテリの取り扱いについて……12
■ 電源の異常……12

本製品について

■機能概要

DAP-2660は、エンタープライズユースに最適の2.4GHz/5GHz デュアルバンド同時利用対応アクセスポイントです。
IEEE 802.11acに対応しています。



■本製品の特長

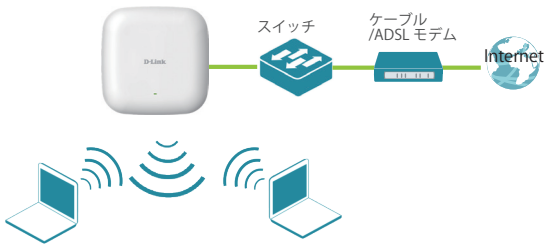
- IEEE 802.11a/b/g/n/ac 準拠
- デュアルバンド通信(2.4GHz/5GHz同時利用)
- WPA/WPA2 Enterprise/Personal暗号方式
- 64/128 ビットWEP 暗号化
- MAC アドレスフィルタリング
- ARP スプーフィング防止
- マルチSSID(周波数帯ごと8個)
- SNMPv1/v2c/v3
- QoS (WMM 準拠)
- AP Array
- GUI、SSL、SSH、Telnetによる設定/ 管理
- 4つの通信モード

■本製品の接続モード

本製品には以下の4つの接続モードがあります。

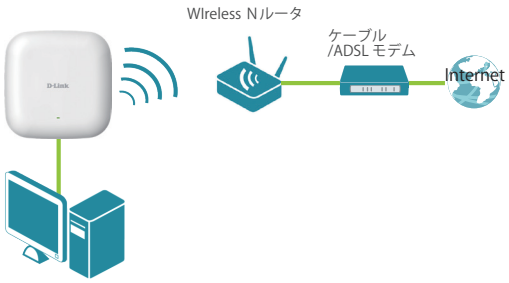
■アクセスポイントモード

無線アクセスポイントと無線クライアントのネットワークを構築します。



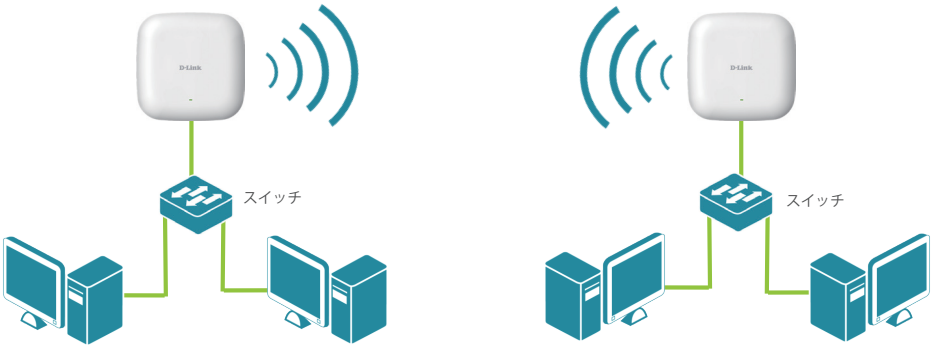
■ワイヤレスクライアントモード

イーサネット用機器向けの無線ネットワークアダプタとして動作します。



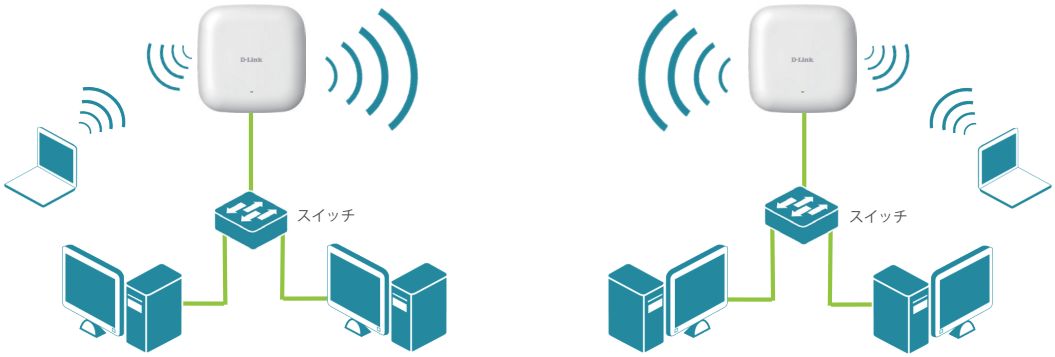
■WDS モード

複数のネットワークを無線接続します。



■WDS with AP モード

無線 LAN アクセスポイントとして動作しながら、複数のネットワークと無線接続します。



■無線LANについて

業界標準に基づく弊社の無線LAN 製品は、ご家庭や職場または公共の施設において、使いやすく互換性の高い高速の無線接続を提供します。これらを使用して時間や場所に関わらず必要なデータにアクセスすることができます。
WLAN は家庭やオフィス環境のみならず、空港やコーヒーショップ、または大学など公共の施設においても幅広く利用されるようになってきました。

このWLAN 技術を用いることにより、仕事やコミュニケーションがさらに効率的に行えるようになってきています。無線技術により可動性が増し、配線や固定のインフラが減少したことでユーザに大きなメリットが生まれました。
ノート型やデスクトップ型PC に使用する無線アダプタはイーサネットのアダプタカードと同じプロトコルをサポートしており、無線ユーザは有線ネットワークと同じアプリケーションを利用できるようになりました。

WLAN 技術を利用するさまざまな理由

- 可動性
  WLAN の動作範囲内のどこからでもデータにアクセス可能であり、生産性を向上します。また、リアルタイムな情報に基づく管理により作業効率が向上します。
- 低い実現コスト
  WLAN は設置、管理、変更、移転のすべてが簡単です。このようなWLAN の扱いやすさはネットワークの変更が頻繁に要求される環境に適しています。WLAN は有線ネットワークでは困難であった場所へのネットワーク導入を可能にします
- 簡単な設置と拡張
  煩わしい複雑なケーブル配線作業、特に壁や天井へのケーブル敷設の必要がないため、手早く簡単にシステムの設置を行うことができます。無線技術は、ネットワークを家庭やオフィスを超えて拡張することで、さらなる多用途性を提供します。
- 低コストのソリューション
  無線LAN デバイスは、従来のイーサネット用機器とほぼ同等の価格設定となっています。本製品は設定可能な4 つのモードで多機能性を提供し、コスト削減を行います。
- 柔軟性
  配置する無線LAN デバイスの数によって、ピアツーピアのネットワークが適している小さなユーザグループから大規模なインフラネットワークまで、自由自在に構築することができます。

世界基準対応の技術

DAP-2660無線アクセスポイントは、IEEE 802.11b、IEEE 802.11g、IEEE 802.11n およびIEEE 802.11acに準拠しています。

IEEE 802.11ac 規格の無線通信速度は、最大866.7bps までと高速化されており、5GHz 帯の周波数と「OFDM」技術をサポートしています。

IEEE 802.11n 規格は、従来のIEEE 802.11a、IEEE 802.11b およびIEEE 802.11g の機能を拡張した規格です。無線通信速度は、最大300Mbps までと高速化され、2.4GHz 帯および5GHz 帯の周波数を利用し、こちらも「OFDM」技術をサポートしています。

これらにより、多くの環境化において、無線サービスエリア内でネットワークによる大容量の送受信や遅延の少ないMPEG 形式の映像の視聴などが可能になります。OFDM(Orthogonal Frequency Division Multiplexing) という技術により、この大容量のデジタルデータの高速伝送を無線で行うことができます。OFDM では、無線信号を小さいサブ信号に分割し、それらを同時に異なる周波数で送信します。OFDM により、信号伝送時のクロストーク（干渉）の発生を抑えることが可能です。

本製品は自動的に最適な通信速度を検出し、高速で広範囲の通信エリアを確保します。

IEEE 802.11n 規格は、「WPA」を含む現在最も先進的なネットワークセキュリティ機能を提供します。
WPA/WPA2 には企業向けの「 Enterprise」とホームユーザ向けの「Personal」の2 種類があります。「WPA-Personal」と「WPA2-Personal」はユーザ認証に必要なサーバ機器を持たないホームユーザを対象としています。その認証方法は、無線ルータやアクセスポイントに「 Pre-Shared Key（ 事前共有鍵）」の定義を行うという点でWEP と似ています。クライアントとアクセスポイントの両方において、事前共有鍵が確認され条件が満たされた時にアクセスが認められます。暗号化には、パケット単位の動的なハッシングを行う「 TKIP（ Temporal Key Integrity Protocol）」と呼ばれる方式を採用しています。また、インテグリティチェック機能により無線通信時のデータの改ざんを防止します。

「WPA-Enterprise」と「 WPA2-Enterprise」は既にセキュリティ用にインフラが整備されている企業を対象としています。ネットワーク内のサーバを中心にネットワーク管理とセキュリティの実施を行うような環境を想定しています。

ネットワーク管理者は、RADIUS サーバ上で802.1X を使用し、無線LAN へのアクセスを許可するユーザのリストを定義します。「WPA-Enterprise」または「 WPA2-Enterprise」を実装した無線LAN にアクセスする場合、ユーザはユーザ名とパスワードの入力を要求されます。ユーザがネットワーク管理者によってアクセスを許可されており、正しいユーザ名とパスワードを入力すると、ネットワークへのアクセスが可能になります。例えば、ある社員が会社を辞めるというような場合、ネットワーク管理者がアクセス許可者のリストからその社員のデータを削除すれば、ネットワークを危険にさらすことは避けることができます。

EAP（ Extensible Authentication Protocol） はWindows OSに実装されています。802.1X の機能を使用する際には、ネットワークにおけるすべてのデバイスのEAP タイプを同一にする必要があります。

重要

最大の無線信号速度は理論値であり、実際のデータスループットは異なります。ネットワーク条件と環境には、ネットワークトラフィック量、建築材料や工事、ネットワークオーバヘッドが含まれ、実際のデータスループット速度は低くなります。環境条件は無線信号範囲に悪影響を与えます。

本マニュアルについて

■マニュアルの構成

1章：お使いになるまえに
本マニュアルの紹介と、本製品をお使いになる前の注意事項を記載しています。
→『お使いになるまえに：p.4 』

2章：設置のしかた
本製品の各部名称と設置方法について説明します。
→『設置のしかた：p.13 』

3章：WEB GUI画面について
WEB GUIへのログイン方法と画面構成について説明します。
→『WEB GUI 画面について：p.20 』

4章：Basic Settings（基本設定）
アクセスポイントの無線モードやセキュリティなど、基本的な設定について説明します。
→『Basic Settings (基本設定)：p.23 』

5章：Advanced Settings（基本設定）
マルチSSIDやVLAN、キャプティブポータルなど、アクセスポイントの詳細設定について説明します。
→『Advanced Settings (詳細設定)：p.36 』

6章：Status（ステータス）
ファームウェアバージョンやクライアント情報、ログなど、ステータスの確認方法について説明します。
→『Status (ステータス)：p.70 』

7章：管理メニュー
本製品の再起動やファームウェアアップデート、設定のリセットなど、管理を行う方法を説明します。
→『管理メニュー：p.78 』

8章：付録
製品を向上出荷時の設定に戻す方法と、FWAQ（よくご質問いただく内容）について記載しています。
→『付録：p.89 』

■マニュアルの対象者

本マニュアルは、本製品の設置および管理についての情報を記載しています。また、ネットワーク管理の概念や用語に十分な知識を持っているネットワーク管理者を対象としています。

■表記規則

本マニュアルでは以下の記号を使用します。

⚠警告 この表示を無視し、間違った使い方をすると、火災や感電などにより人身事故になるおそれがあります。

⚠注意 この表示を無視し、間違った使い方をすると、傷害または物損損害が発生するおそれがあります。

（重要） 設定の組み合わせ、イベントや手順によりネットワークの接続状態やセキュリティなどに悪影響を及ぼす恐れのある事項について説明します。

（メモ） 特長や技術についての詳細情報を記述します。

本マニュアル中での字体、・記号についての表記規則は以下のとおりです。

字体	解説	例
『水色』	マニュアル内の参照先	『Basic Settings (基本設定)：p.23 』

安全にお使いいただくために

ご自身の安全を確保し、システムを破損から守るために、以下に記述する安全のための指針をよくお読みください。

安全上のご注意　必ずお守りください

本製品を安全にお使いいただくために、以下の項目をよくお読みになり必ずお守りください。

⚠警告	この表示を無視し、間違った使い方をすると、火災や感電などにより人身事故になるおそれがあります。
⚠注意	この表示を無視し、間違った使い方をすると、傷害または物損損害が発生するおそれがあります。

記号の意味　⃠ してはいけない**「禁止」**内容です。　❗ 必ず実行していただく**「指示」**の内容です。

⚠警告

分解禁止　分解・改造をしない
機器が故障したり、異物が混入すると、やけどや火災の原因となります。

禁止　落としたり、重いものを乗せたり、強いショックを与えたり、圧力をかけたりしない
故障の原因につながります。

禁止　発煙、焦げ臭い匂いの発生などの異常状態のまま使用しない
感電、火災の原因になります。
使用を止めて、ケーブル / コード類を抜いて、煙が出なくなってから販売店に修理をご依頼してください。

ぬれ手禁止　ぬれた手でさわらない
感電のおそれがあります。

水ぬれ禁止　水をかけたり、ぬらしたりしない
内部に水が入ると、火災、感電、または故障のおそれがあります。

禁止　油煙、湯気、湿気、ほこりの多い場所、振動の激しいところでは使わない
火災、感電、または故障のおそれがあります。

禁止　内部に金属物や燃えやすいものを入れない
火災、感電、または故障のおそれがあります。

禁止　表示以外の電圧で使用しない
火災、感電、または故障のおそれがあります。

禁止　たこ足配線禁止
たこ足配線などで定格を超えると火災、感電、または故障の原因となります。

禁止　設置、移動のときは電源プラグを抜く
火災、感電、または故障のおそれがあります。

禁止　雷鳴が聞こえたら、ケーブル / コード類にはさわらない
感電のおそれがあります。

禁止　ケーブル / コード類や端子を破損させない
無理なねじり、引っ張り、加工、重いものの下敷きなどは、ケーブル / コードや端子の破損の原因となり、火災、感電、または故障につながります。

禁止　正しい電源ケーブル、コンセントを使用する
火災、感電、または故障の原因となります。

禁止　乳幼児の手の届く場所では使わない
やけど、ケガ、または感電の原因になります。

禁止　次のような場所では保管、使用をしない
・直射日光のあたる場所
・高温になる場所
・動作環境範囲外

禁止　光源をのぞかない
光ファイバケーブルの断面、コネクタ、および製品のコネクタをのぞきますと強力な光源により目を損傷するおそれがあります。

⚠注意

❗　静電気注意
コネクタやプラグの金属端子に触れたり、帯電したものを近づけますと故障の原因となります。

❗　コードを持って抜かない
コードを無理に曲げたり、引っ張りますと、コードや機器の破損の原因となります。

❗　振動が発生する場所では使用しない
接触不良や動作不良の原因となります。

禁止　付属品の使用は取扱説明書にしたがう
付属品は取扱説明書にしたがい、他の製品には使用しないでください。機器の破損の原因になります。

電波障害自主規制について

この装置は、クラスB 情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。

VCCI-B

無線に関するご注意

■電波に関するご注意

本製品は、電波法に基づく小電力データ通信システムの無線製品として、技術基準適合証明を受けています。従って、本製品の使用する上で、無線局の免許は必要ありません。
本製品は、日本国内でのみ使用できます。
以下の注意をよくお読みになりご使用ください。

◎ この機器を以下の場所では使用しないでください。
- 心臓ペースメーカー等の産業・科学・医療用機器の近くで使用すると電磁妨害を及ぼし、生命の危険があります。
- 工場の製造ライン等で使用されている移動体識別用の構内無線局(免許を必要とする無線局) および特定小電力無線局(免許を必要としない無線局)
- 電子レンジの近くで使用すると、電子レンジによって無線通信に電磁妨害が発生します

◎ 本製品は技術基準適合証明を受けています。本製品の分解、改造、および裏面の製品ラベルをはがさないでください。

■2.4GHz 帯使用の無線機器の電波干渉に関するご注意

本製品の使用周波数帯では、電子レンジ等の産業・科学・医療用機器のほか工場の製造ライン等で使用している移動体識別用の構内無線局(免許を必要とする無線局) および特定小電力無線局(免許を必要としない無線局) 並びにアマチュア無線局(免許を必要とする無線局) が運用されています。

◎ この機器を使用する前に、近くで移動体識別用の構内無線局および特定小電力無線局並びにアマチュア無線局が運用されていないことを確認してください。

◎ 万一、この機器から移動体識別用の構内無線局に対して有害な電波干渉の事例が発生した場合には、速やかに使用周波数を変更するか、または電波の発射を停止してください。

◎ その他、この機器から移動体通信用の特定小電力無線局に対して電波干渉の事例が発生した場合など、何かお困りのことが起きたときは、弊社サポート窓口へお問い合わせください。

使用周波数帯域	2.4GHz 帯
変調方式	DS-SS 方式/OFDM 方式
想定干渉距離	40m以下
周波数変更可否	全帯域を使用し、かつ移動体識別用の構内無線局および特定小電力無線局並びにアマチュア無線局の帯域を回避可能

■無線LAN 製品ご使用時におけるセキュリティに関するご注意

無線LAN では、LAN ケーブルを使用する代わりに、電波を利用してパソコン等と無線アクセスポイント間で情報のやり取りを行うため、電波の届く範囲であれば自由にLAN 接続が可能であるという利点があります。
その反面、電波はある範囲内であれば障害物 (壁等) を越えてすべての場所に届くため、セキュリティに関する設定を行っていない場合、以下のような問題が発生する可能性があります。

◎ 通信内容を盗み見られる
悪意ある第三者が、電波を故意に傍受し、以下の通信内容を盗み見られる可能性があります。
- ID やパスワード又はクレジットカード番号等の個人情報
- メールの内容

◎ 不正に侵入される
悪意ある第三者が、無断で個人や会社内のネットワークへアクセスし、以下の行為を行う可能性があります。
- 個人情報や機密情報を取り出す (情報漏洩)
- 特定の人物になりすまして通信し、不正な情報を流す (なりすまし)
- 傍受した通信内容を書き換えて発信する (改ざん)
- コンピュータウィルスなどを流しデータやシステムを破壊する (破壊)

本来、無線LAN カードや無線アクセスポイントは、これらの問題に対応するためのセキュリティの仕組みを持っていますので、無線LAN 製品のセキュリティに関する設定を行って製品を使用することで、その問題が発生する可能性は少なくなります。

セキュリティの設定を行わないで使用した場合の問題を充分理解した上で、お客様自身の判断と責任においてセキュリティに関する設定を行い、製品を使用することをお奨めします。

ご使用上の注意

けがや感電、火災および装置の破損のリスクを減らすために、以下の注意事項を遵守してください。

◎ 保守マーク表示を守ってください。また、ドキュメント類に説明されている以外の方法でのご使用はやめてください。三角形の中に稲妻マークがついたカバー類をあけたり外したりすると、感電の危険性を招きます。筐体の内部は、訓練を受けた保守技術員が取り扱うようにしてください。

◎ 以下のような状況に陥った場合は、電源ケーブルをコンセントから抜いて、部品の交換をするかサービス会社に連絡してください。
- 電源ケーブル、延長ケーブル、またはプラグが破損した。
- 製品の中に異物が入った。
- 製品に水がかかった。
- 製品が落下した、または損傷を受けた。
- 操作方法に従って運用しているのに正しく動作しない。

◎ 本製品をラジエータや熱源の近くに置かないでください。また冷却用通気孔を塞がないようにしてください。

◎ 食べ物や飲み物が本製品にかからないようにしてください。また、水気のある場所での運用は避けてください。万一製品が濡れてしまった場合は、トラブルシューティングガイドの該当する文をお読みになるか、サービス会社に連絡してください。

◎ 本システムの開口部に物を差し込まないでください。内部コンポーネントのショートによる火事や感電を引き起こすことがあります。

◎ 本製品と一緒にその他のデバイスを使用する場合は、弊社の認定を受けたデバイスを使用してください。

◎ カバーを外す際、あるいは内部コンポーネントに触れる際は、製品の温度が十分に下がってから行ってください。

◎ 電気定格ラベル標記と合致したタイプの外部電源を使用してください。正しい外部電源タイプがわからない場合は、サービス会社、あるいはお近くの電力会社にお問い合わせください。

◎ システムの損傷を防ぐために、電源装置の電圧選択スイッチ（装備されている場合のみ）がご利用の地域の設定と合致しているか確認してください。
- 東日本では100V/50Hz、西日本では100V/60Hz

◎ また、付属するデバイスが、ご使用になる地域の電気定格に合致しているか確認してください。

◎ 付属の電源ケーブルのみを使用してください。

◎ 感電を防止するために、本システムと周辺装置の電源ケーブルは、正しく接地された電気コンセントに接続してください。このケーブルには、正しく接地されるように、3 ピンプラグが取り付けられています。アダプタプラグを使用したり、ケーブルから接地ピンを取り外したりしないでください。延長コードを使用する必要がある場合は、正しく接地されたプラグが付いている3 線式コードを使用してください。

◎ 延長コードと電源分岐回路の定格を守ってください。延長コードまたは電源分岐回路に差し込まれているすべての製品の合計定格アンペア数が、その延長コードまたは電源分岐回路の定格アンペア限界の8 割を超えないことを確認してください。

◎ 一時的に急激に起こる電力の変動からシステムコンポーネントを保護するには、サージサプレッサ、回線調整装置、または無停電電源装置（UPS）を使用してください。

◎ ケーブルと電源コードは慎重に取り付けてください。踏みつけられたりつまずいたりしない位置に、ケーブルと電源コードを配線し、コンセントに差し込んでください。また、ケーブル上に物を置いたりしないようにしてください。

◎ 電源ケーブルやプラグを改造しないでください。設置場所の変更をする場合は、資格を持った電気技術者または電力会社にお問い合わせください。国または地方自治体の配線規則に必ず従ってください。

◎ システムに対応しているホットプラグ可能な電源装置に電源を接続したり、切り離したりする際には、以下の注意を守ってください。
- 電源装置を取り付ける場合は、電源装置を取り付けてから、電源ケーブルを電源装置に接続してください。
- 電源装置を取り外す場合は、事前に電源ケーブルを抜いておいてください。
- システムに複数の電源がある場合、システムから電源を切り離すには、すべての電源ケーブルを電源装置から抜いてください。

◎ 製品の移動は気をつけて行ってください。キャスタやスタビライザがしっかり装着されているか確認してください。急停止や、凹凸面上の移動は避けてください。

静電気障害を防止するために

静電気は、システム内部の精密なコンポーネントを損傷する恐れがあります。静電気による損傷を防ぐため、マイクロプロセッサなどの電子部品に触れる前に、身体から静電気を逃がしてください。シャーシの塗装されていない金属面に定期的に触れることにより、身体の静電気を逃がすことができます。

さらに、静電気放出（ESD）による損傷を防ぐため、以下の手順を実行することをお勧めします。

1. 静電気に敏感なコンポーネントを箱から取り出す時は、コンポーネントをシステムに取り付ける準備が完了するまで、コンポーネントを静電気防止包装から取り出さないでください。静電気防止包装から取り出す直前に、必ず身体の静電気を逃してください。
2. 静電気に敏感な部品を運ぶ場合、最初に静電気防止容器またはパッケージに入れてください。
3. 静電気に敏感なコンポーネントの取り扱いは、静電気のない場所で行います。可能であれば、静電気防止床パッド、作業台パッド、および帯電防止接地ストラップを使用してください。

バッテリの取り扱いについて

⚠警告

不適切なバッテリの使用により、爆発などの危険性が生じることがあります。バッテリの交換は、必ず同じものか、製造者が推奨する同等の仕様のものをご使用ください。バッテリの廃棄については、製造者の指示に従って行ってください。

電源の異常

万一停電などの電源異常が発生した場合は、必ず本スイッチの電源プラグを抜いてください。電源が再度供給できる状態になってから電源プラグを再度接続します。

設置のしかた

2

本製品の各部名称や、設置する際の準備・方法について説明します。
設置を行う際にお読みください。

■ パッケージの内容 14
■ 動作環境 14
■ ネットワーク接続前の準備 14
設置にあたってのご注意 14
■ 本体各部名称 15
前面パネル 15
背面パネル 15
■ 製品の設置 16
イーサネットケーブルの接続 16
ACアダプタの接続 16
接続例 16
PoEを使用しない接続 16
PoEスイッチ/PoEルータを使用したPoE接続 16
マウントキットによる設置 17
マウントプレートを使用して取り付ける 17
天井ブラケットを使用して取り付ける 18
■ アクセスポイント設置後のネットワーク接続の例 19

パッケージの内容

本製品には、以下のものが同梱されています。

- 本体
- ACアダプタ
- ネットワークケーブル
- マウントキット
- マニュアル
- シリアルラベル
- CD-ROM
- ゴム足

不足しているものや損傷を受けているものがありましたら、弊社ホームページにてユーザ登録を行い、サポート窓口までご連絡ください。

動作環境

本製品の動作には、以下の環境が必要です。

- 以下のブラウザをサポートしているコンピュータ
  - Microsoft Internet Explorer 7.0 以降
  - Mozilla Firefox 3.5 以降
  - Apple Safari 5.0 以降
  - Google Chrome 20 以降

- イーサネットへの接続

ネットワーク接続前の準備

アクセスポイントの設置場所が性能に大きな影響を与えます。以下の注意事項に従って本製品を設置してください。

● 設置にあたってのご注意

本製品の使用により、動作範囲内にて無線でネットワークアクセスが可能になります。
しかし、壁や天井など、無線信号が通過する物体の数や厚さ・場所などにより、動作範囲が制約を受ける場合があります。
一般的には、構造物の材質や設置場所での無線周波数のノイズが動作範囲に影響を与えます。

◎ 本製品と他のネットワークデバイスとの間に入る壁や天井の数をできるだけ少なくしてください。一枚の壁や天井の影響により、本製品の動作範囲は1 ～ 30 メートルの範囲となります。間に入る障害物の数を減らすようデバイスの位置を工夫してください。

◎ ネットワークデバイス間の直線距離にご注意ください。厚さ50 センチの壁を45 度の角度で無線信号が通過する時、通り抜ける壁の厚みは約1メートルになります。2 度の角度で通過すると、通り抜ける厚みは14 メートルになります。信号が障害物をなるべく直角に通過するような位置にデバイスを設置し、電波を受信しやすくしてください。

◎ 無線信号の通過性能は建築材料により異なります。金属製のドアやアルミの金具などは動作範囲を小さくする可能性があります。無線LAN デバイスや無線LAN アダプタ使用のコンピュータの設置は、信号がなるべく乾式壁か開放された戸口などを通るような位置に設置してください。

◎ 周波数ノイズを発生する電気機器や家電製品からは、最低でも1、2 メートル離してデバイスを設置してください。

◎ 2.4GHz のコードレス電話またはX-10（シーリングファン、ライト、およびホームセキュリティシステムなどの無線製品）を使っている場合、ご使用の無線接続は著しく性能が低下するか、または完全に切断される可能性があります。2.4GHz 電話の親機は可能な限りご使用の無線機器から離れていることを確認してください。電話を使用していない場合でも、親機は信号を送信します。

◎ 必ず付属のUTP ケーブル、AC アダプタをご使用ください。

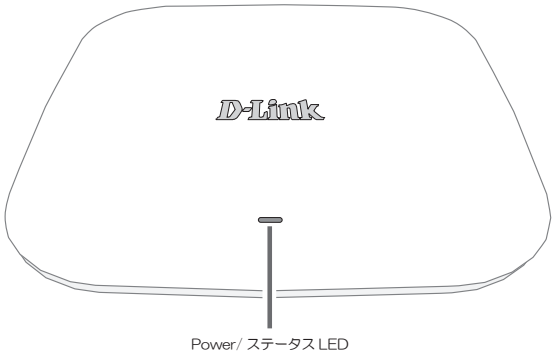
⚠注意

本アクセスポイントは、IEEE 802.3af 準拠の給電スイッチまたは弊社が承認する給電機器から受電することができます。弊社が承認していないPoE 給電機器に本アクセスポイントを接続すると、本アクセスポイントが破損する場合があります。

本体各部名称

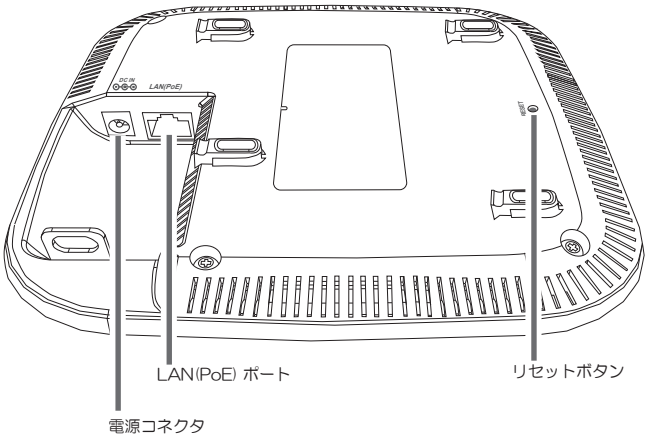
アクセスポイントの各部名称について説明します。

■前面パネル



LED	色	状態	状況説明
POWER/ ステータス LED	緑	点灯	動作中です。 正しく起動しました。
		点滅	ネットワーク上でデータを送受信しています。
	赤	点灯	起動に失敗しました。
		点滅	起動中です。 または不具合が発生しています。

■背面パネル



名称	説明
LAN (PoE) ポート (10BASE-T/100BASE-TX/1000BASE-T)	RJ-45ケーブルを挿入し、ネットワークへの接続を行います。 (メモ) PoE による受電を行うこともできます。
リセットボタン	本製品を工場出荷時設定にリセットします。
電源コネクタ	付属のAC アダプタを接続します。 (メモ) PoE による受電を行う場合は接続する必要がありません。

製品の設置

■イーサネットケーブルの接続

1. イーサネットケーブルの一端を、本製品の背面にある RJ-45 コネクタに接続します。
2. イーサネットケーブルのもう一端を、ルータ／スイッチ等のネットワーク機器に接続します。

■ACアダプタの接続

付属のACアダプタを使用して、本製品に電源を投入します。

1. 付属の AC アダプタを本製品に接続します。
2. AC アダプタのプラグを電源コンセントに接続します。

メモ

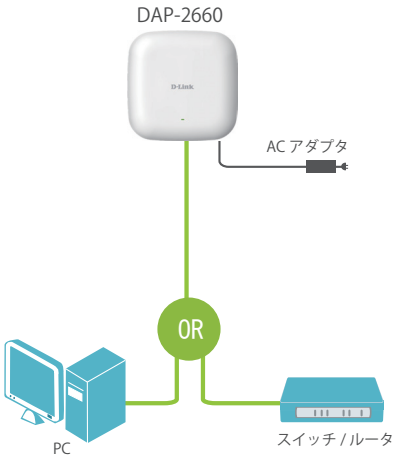
本スイッチに電源が供給されると、POWER/ステータス LED が点灯します。

■接続例

本製品に電源を接続するには以下の方法があります。

● PoEを使用しない接続

1. イーサネットケーブルで、本製品とスイッチ／ルータまたは PC を接続します。
2. 付属の AC アダプタを本製品に接続します。
3. AC アダプタのプラグを電源コンセントに接続します。



● PoEスイッチ/PoEルータを使用したPoE接続

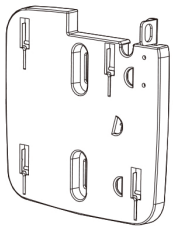
1. イーサネットケーブルで、本製品と PoE スイッチ /PoE ルータを接続します。

■マウントキットによる設置

本製品は、マウントキットを使用して壁面や天井に設置することができます。
設置の際は以下の手順を参照してください。

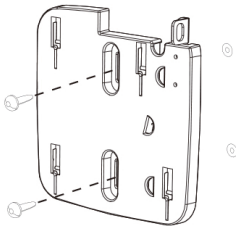
● マウントプレートを使用して取り付ける

1. アクセスポイントを取り付ける壁または天井にマウントプレートを合わせます。

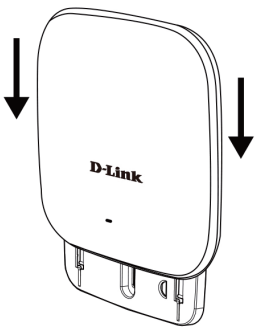


2. アンカーをつける場所にマークをつけます。
3. マークした場所に穴をあけ、プラスティックのアンカーを挿入します。

4. アンカー用のネジを使用し、マウントプレートを壁面に取り付けます。

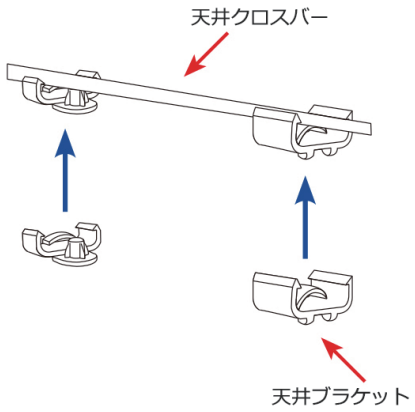


5. アクセスポイントの LAN ポートにイーサネットケーブルを挿入します。
6. マウントプレートにアクセスポイントを取り付けます。

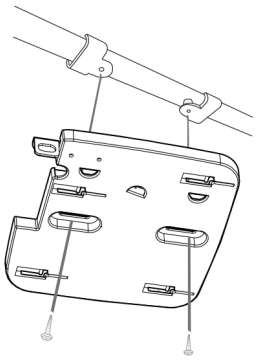


● 天井ブラケットを使用して取り付ける

1. 天井のパネルに 2 つの天井ブラケットを挟みます。
両方のブラケットが直線になっていることを確認してください。

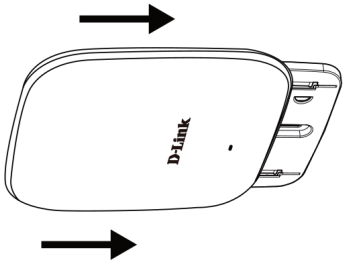


2. 同梱されているネジを使用し、天井ブラケットにマウントプレートを取り付けます。



3. アクセスポイントの LAN ポートにイーサネットケーブルを挿入します。

4. マウントプレートにアクセスポイントを取り付けます。

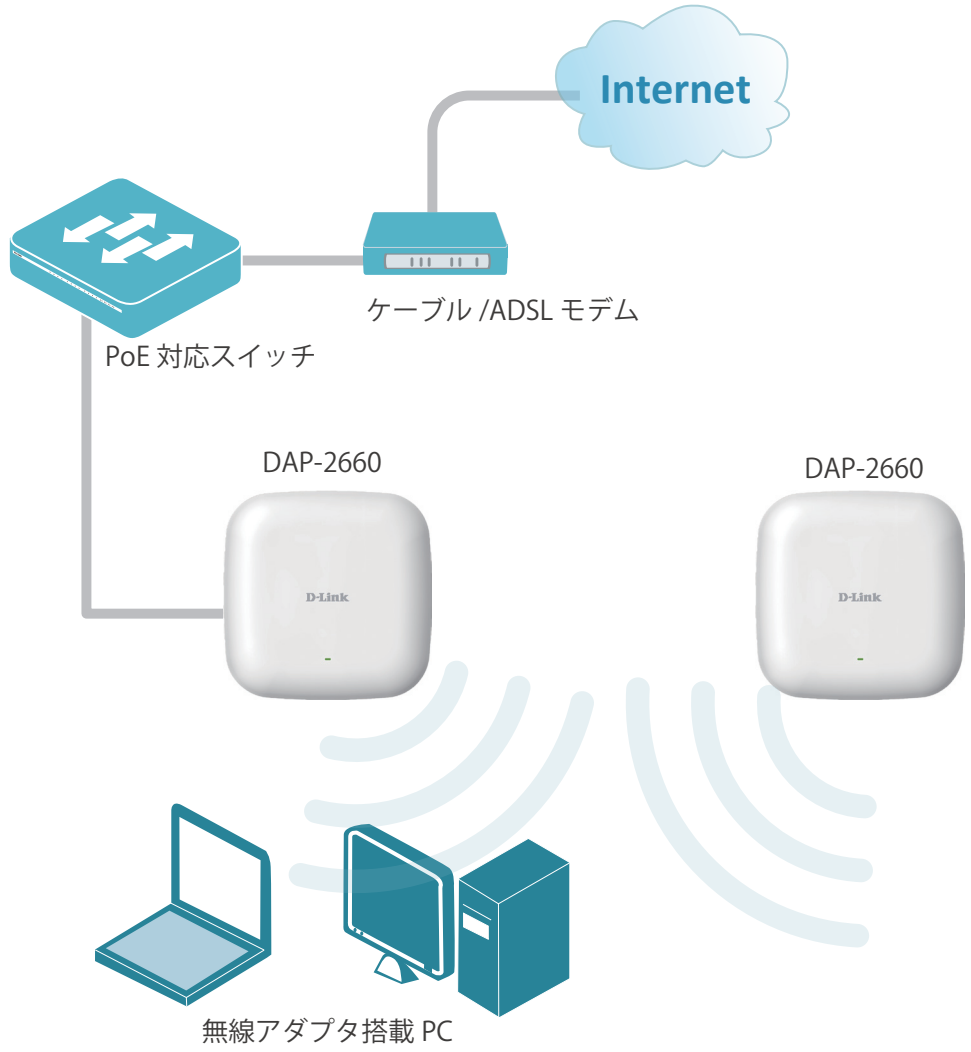


アクセスポイント設置後のネットワーク接続の例

1. インターネット接続を確認します。
2. ご契約のプロバイダに確認し、正しくモデムを設置します。
3. ケーブルモデムまたは ADSL モデムをルータに接続します。接続に関する詳細については、ルータに付属の設置マニュアルを参照してください。

◆ **デスクトップ型コンピュータへの接続を行う場合：**
無線アダプタをそれぞれのインタフェースに従って、空いているPCI スロット、USB ポートなどに差し込み、必要に応じてドライバをインストールしてください。

◆ **ノート型コンピュータへの接続を行う場合：**
無線アダプタをそれぞれのインタフェースに従って、空いているカードバススロット、USB ポートなどに差し込み、必要に応じてドライバをインストールしてください。



WEB GUI 画面について 3

本製品は、WEB GUI画面から設定・操作を行うことができます。
WEB GUI画面へのログイン方法と画面構成について説明します。

■ WEB GUI画面へのログイン 21

■ 画面の構成 22

管理メニュー.....22

設定メニュー.....22

メイン画面.....22

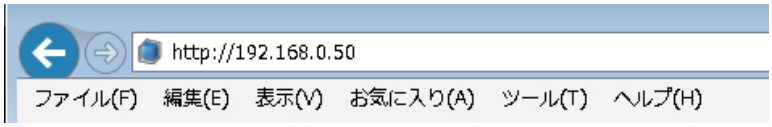
WEB GUI画面へのログイン

メモ

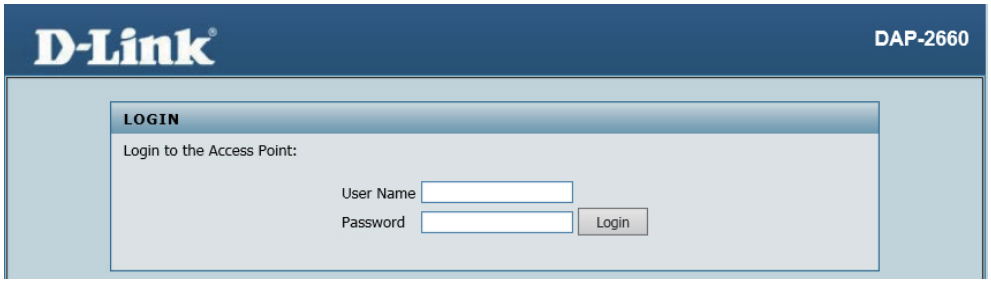
- 本製品の設定は、UTPケーブルで接続したPCから行います。設定を始める前に、本製品とPCをUTPケーブルで接続してください。
- 本製品のIPアドレスとPCのIPアドレスは、同じサブネット内に設定してください。
  例) 本製品のIPアドレス：192.168.0.50、PCのIPアドレス：192.168.0.51
- PCのプロキシサーバ機能は無効にしてください。
  ■手順：
  Windowsの「スタート」>「コントロールパネル」>「インターネットオプション」>「接続」タブ >「LANの設定」の順にクリックし、「LAN にプロキシサーバを使用する」のチェックを外します。

1. Web ブラウザを起動します。

2. Web ブラウザに本製品の IP アドレスを入力します。

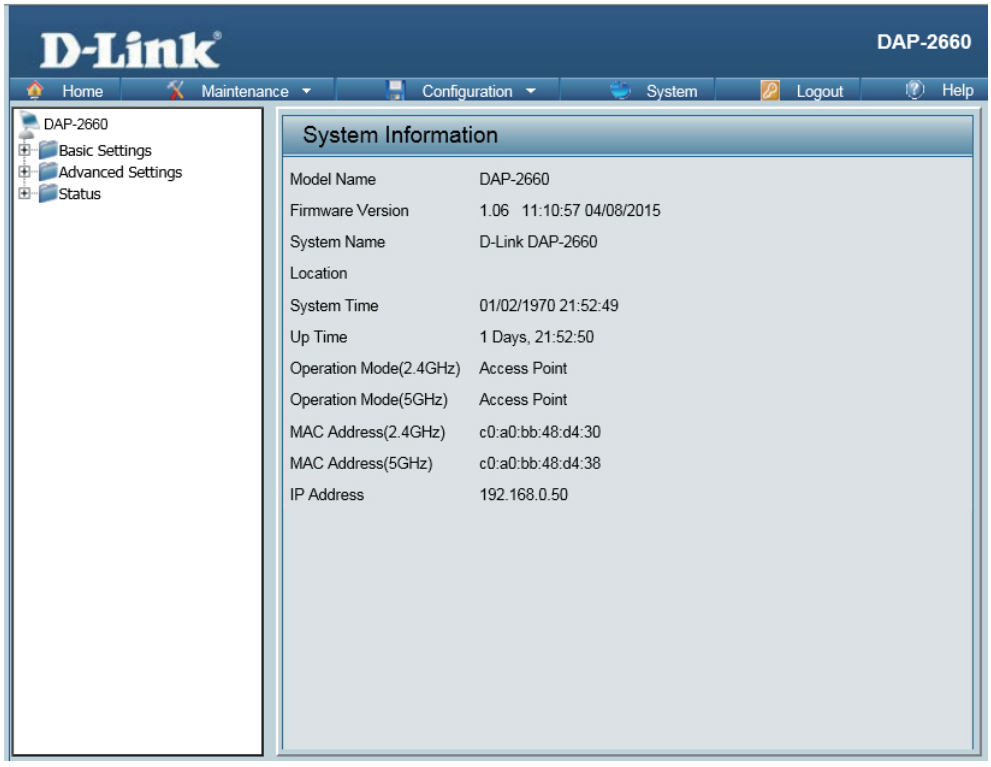


3. 「User Name」と「Password」を入力します。



工場出荷時の設定は以下です。
- User Name：admin
- Password：空欄

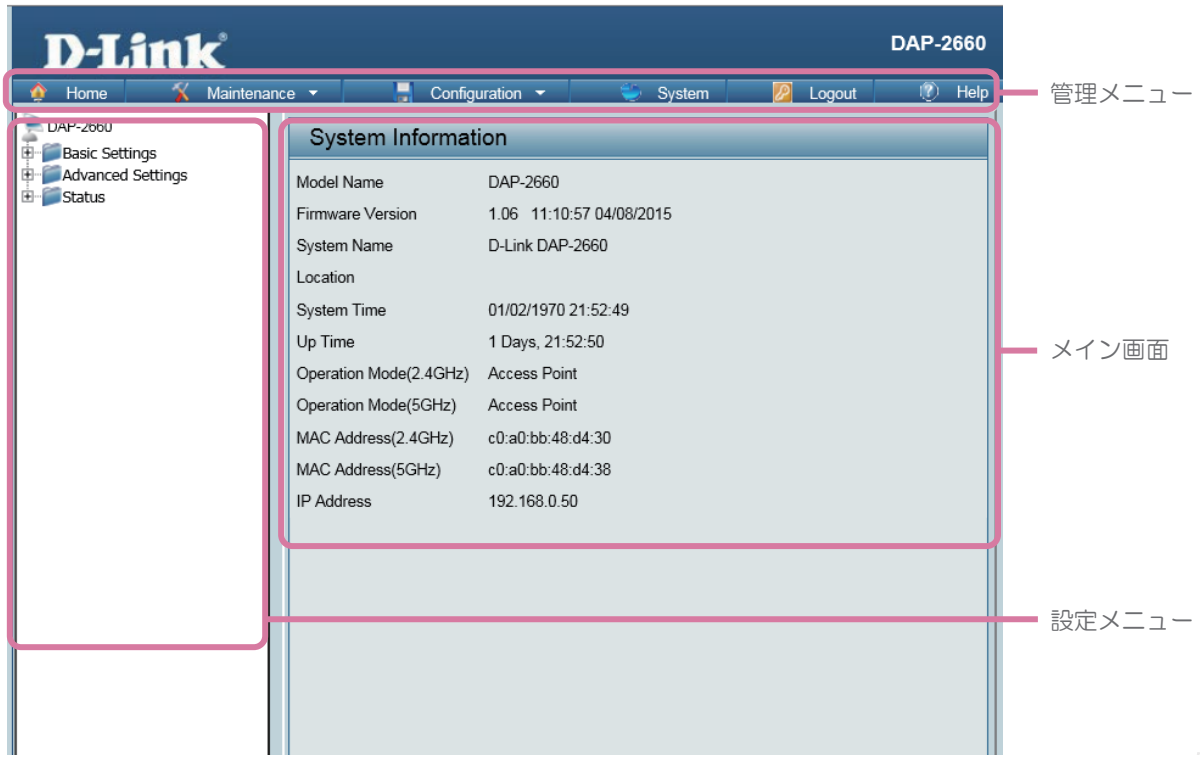
4. 以下の画面が表示されます。



WEB GUIからログアウトする場合は、画面右上の「Logout」からログアウトを行ってください。

画面の構成

WEB GUI画面の構成について説明します。



● 管理メニュー

- Home :
  クリックすると、System Information 画面が表示されます。
- Maintenance :
  管理者権限の設定やファームウェアのアップロードなど、本製品のメンテナンスを行います。
- Configuration :
  設定の保存・取り消しを行います。
- System :
  本製品の再起動・工場出荷時設定へのリセットを行います。
- Logout :
  WEB GUIからのログアウトを行います。
- Help :
  ヘルプ画面が表示されます。

メモ

管理メニューの詳細については、『管理メニュー：p.78 』を参照してください。

● 設定メニュー

アクセスポイントの無線モードやセキュリティなど、各機能の設定を行います。

メモ

設定メニューの詳細については、『Basic Settings (基本設定)：p.23 』『Advanced Settings (詳細設定)：p.36 』『Status (ステータス)：p.70 』を参照してください。

● メイン画面

設定メニューおよび管理メニューで選択した項目の設定画面が表示されます。

Basic Settings（基本設定）

4

アクセスポイントの無線モードやセキュリティなどの設定を行います。

■ Basic Settings について 24

■ Wireless Settings（ワイヤレス設定）..... 24

Access Point モードを選択した場合..... 25

WDSモード／WDS with APモードを選択した場合 26

Wireless Clientモードを選択した場合 28

Authentication（認証）の設定について 30

[Open System] または[Shared Key]を選択した場合.....30

[WPA-Personal]を選択した場合.....31

[WPA-Enterprise]を選択した場合 32

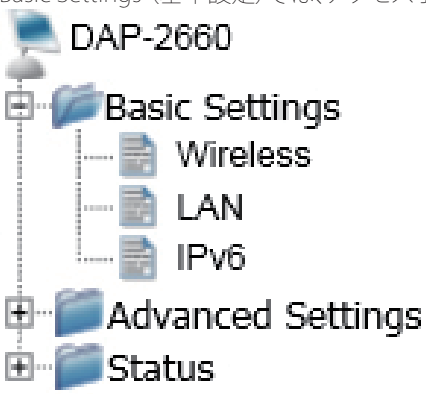
[802.1 X]を選択した場合 33

■ LAN Settings（LAN設定）..... 34

■ IPv6 Settings（IPv6設定）..... 35

Basic Settings について

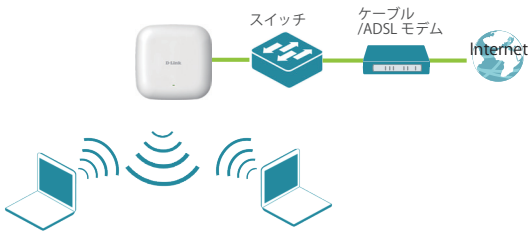
Basic Settings（基本設定）では、アクセスポイントの通信モードの選択やセキュリティ設定、LANの設定などを行います。



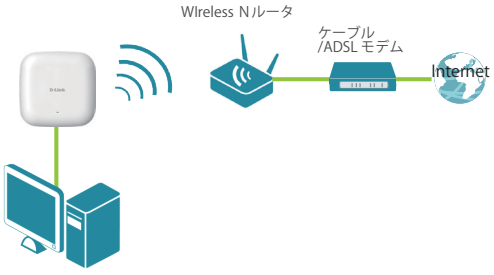
Wireless Settings （ワイヤレス設定）

アクセスポイントの通信モードを選択し、それに応じてネットワーク名（SSID）や認証方法などの設定を行います。
選択できる通信モードは以下の通りです。

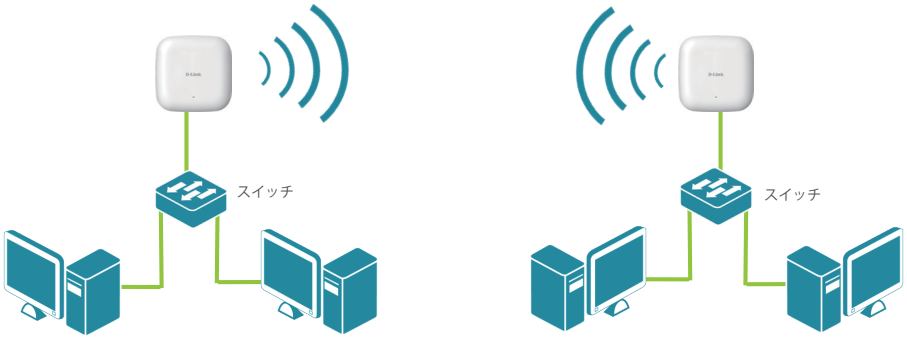
■アクセスポイントモード
無線アクセスポイントと無線クライアントのネットワークを構築します。



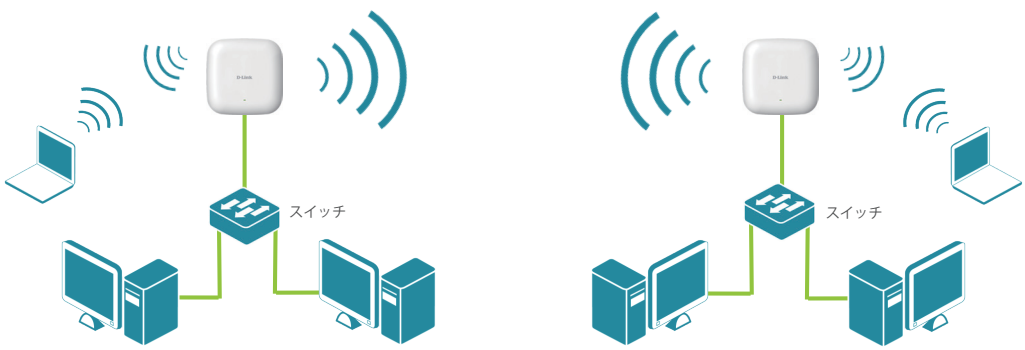
■ワイヤレスクライアントモード
イーサネット用機器向けの無線ネットワークアダプタとして動作します。



■WDS モード
複数のネットワークを無線接続します。



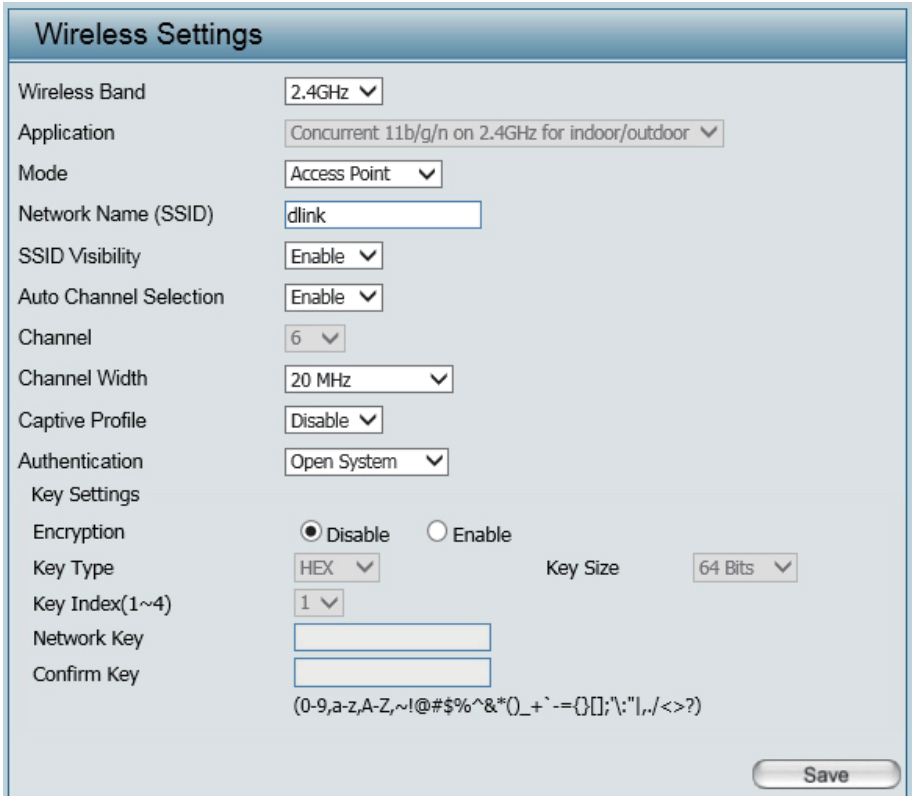
■WDS with AP モード
無線 LAN アクセスポイントとして動作しながら、複数のネットワークと無線接続します。



1. [Basic Settings] > [Wireless] を選択します。
2. [Wireless Band] で周波数帯を [2.4GHz] または [5GHz] に設定します。
3. 周波数帯を [5GHz] に設定した場合は、[Application] を以下から選択します。
   - [Concurrent 11a/n on W52/W53/W56 for indoor]/[Concurrent 11a/n on W56 for indoor]
     周波数帯に[2.4GHz]を選択した場合は、アプリケーション[Concurrent 11b/g/n on2.4GHz for indoor/outdoor]が表示されます。
4. [Mode] で、アクセスポイントの通信モードを以下から選択します。
   - [Access Point] /[WDS with AP]/ [WDS] /[Wirelss Client]
5. 選択した通信モードに応じて必要な設定を行います。
6. 設定完了後、[Save] をクリックします。

■Access Point モードを選択した場合

本製品は無線アクセスポイントとして動作し、無線クライアントとのネットワークを構築します。



◆ **Network Name (SSID)**	ネットワーク名（SSID）を入力します。 ・初期値：[dlink] ・入力可能文字数：32文字以内（大文字と小文字は区別されます。） SSID(Service Set Identifier)とは、無線LANのアクセスポイントを識別するための名前です。無線LANのアクセスポイントが複数ある場合、どのアクセスポイントに接続するかを指定する必要があり、SSIDはその際に使用されます。
◆ **SSID Visibility**	SSIDの表示を有効または無効にします。 ・選択肢：[Enable]（有効）[Disable]（無効） [Enable](有効)に設定すると、SSIDがネットワークにブロードキャストされ、すべてのネットワークユーザがSSIDを閲覧できるようになります。
◆ **Auto Channel Selection**	自動チャネル選択を有効または無効にします。 ・選択肢：[Enable]（有効）[Disable]（無効） [Enable](有効)に設定すると、アクセスポイントが自動的に最適なチャネルを選択します。
◆ **Channel**	[Auto Channel Selection]を無効にした場合に、チャネルを選択します。
◆ **Channel Width**	チャネル帯域を選択します。 ・選択肢：[20MHz][Auto 20/40MHz][Auto 20/40/80MHz] [Auto 20/40/80MHz]は5GHzを選択した場合のみ選択可能です。
◆ **Captive Profile**	Captive Portal Authenticationで設定したプロファイルを選択するか、[Disable](無効)を選択します。
◆ **Authentication**	認証方式を選択します。 ・選択肢：[Open System][Shared Key][WPA-Personal][WPA-Enterprise][802.1X]

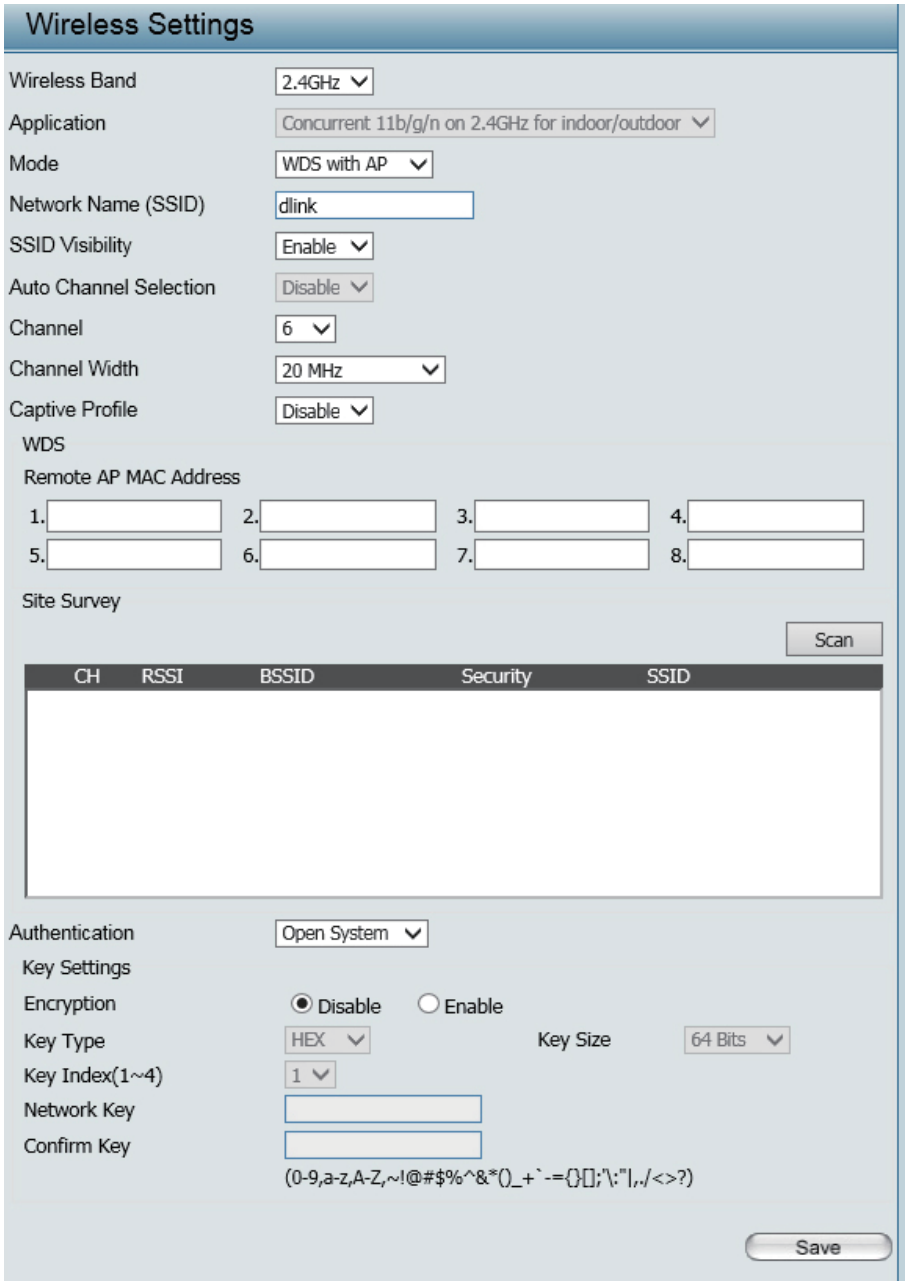
メモ

[Authentication](認証)の設定内容は、選択した方式によって異なります。
詳細は『Authentication (認証) の設定について : p.30 』を参照してください。

■WDSモード／WDS with APモードを選択した場合

WDSモードの場合：
複数のネットワークと無線接続します。

WDS with APモードの場合：
本製品は無線LAN アクセスポイントとして動作しながら、複数のネットワークと無線接続します。



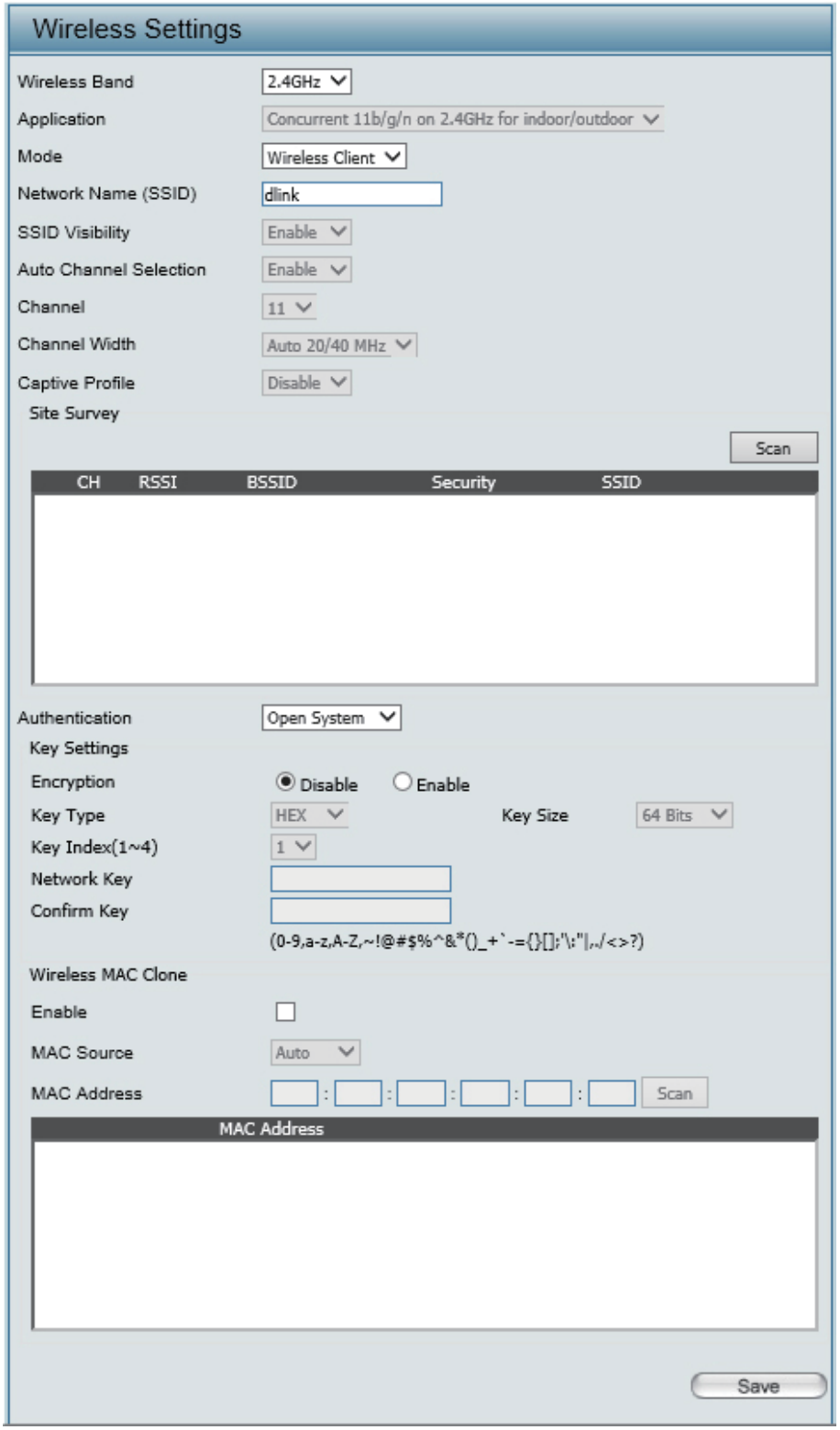
◆ **Mode**	通信モードを選択します。 ・選択肢：[Access Point] [WDS with AP] [WDS] [Wirelss Client]
◆ **Network Name (SSID)**	ネットワーク名（SSID）を入力します。 ・初期値：[dlink] ・入力可能文字数：32文字以内（大文字と小文字は区別されます。） SSID(Service Set Identifier)とは、無線LANのアクセスポイントを識別するための名前です。 無線LANのアクセスポイントが複数ある場合、どのアクセスポイントに接続するかを指定する必要があり、SSIDはその際に使用されます。
◆ **SSID Visibility**	SSIDの表示を有効または無効にします。 ・選択肢：[Enable]（有効）[Disable]（無効） [Enable](有効)に設定すると、SSIDがネットワークにブロードキャストされ、すべてのネットワークユーザがSSIDを閲覧できるようになります。
◆ **Auto Channel Selection**	自動チャネル選択を有効または無効にします。 ・選択肢：[Enable]（有効）[Disable]（無効） [Enable](有効)に設定すると、アクセスポイントが自動的に最適なチャネルを選択します。
◆ **Channel**	[Auto Channel Selection]を無効にした場合に、チャネルを選択します。
◆ **Channel Width**	チャネル帯域を選択します。 ・選択肢：[20MHz][Auto 20/40MHz][Auto 20/40/80MHz] [Auto 20/40/80MHz]は5GHzを選択した場合のみ選択可能です。
◆ **Captive Profile**	キャプティブプロファイルを有効または無効にします。 ・選択肢：[Enable]（有効）[Disable]（無効）
◆ **WDS Remote AP MAC Address**	ネットワーク上にある対向のアクセスポイントのMACアドレスを入力します。
◆ **Site Survey**	[Scan]をクリックしてサイトサーベイを実行します。 サイトサーベイを実行すると、稼働中のアクセスポイントが検出され、表示されます。
◆ **Authentication**	認証方式を選択します。 ・選択肢：[Open System][WPA-Personal]

メモ

[Authentication](認証方式)の設定内容は、選択した方式によって異なります。
詳細は『Authentication（認証）の設定について：p.30 』を参照してください。

■Wireless Clientモードを選択した場合

本製品は、イーサネット機器用の無線ネットワークアダプタとして動作します。



◆ **Mode**	通信モードを選択します。 ・選択肢：[Access Point] [WDS with AP] [WDS] [Wirelss Client]
◆ **Network Name (SSID)**	通信モードに[Wireless Client]を選択した場合は設定できません。
◆ **SSID Visibility**	通信モードに[Wireless Client]を選択した場合は設定できません。
◆ **Auto Channel Selection**	通信モードに[Wireless Client]を選択した場合は設定できません。
◆ **Channel**	通信モードに[Wireless Client]を選択した場合は設定できません。
◆ **Channel Width**	通信モードに[Wireless Client]を選択した場合は設定できません。
◆ **Captive Profile**	通信モードに[Wireless Client]を選択した場合は設定できません。
◆ **Site Survey**	[Scan]をクリックしてサイトサーベイを実行します。 サイトサーベイを実行すると、稼働中のアクセスポイントが検出され、表示されます。
◆ **Authentication**	認証方式を選択します。 ・選択肢：[Open System][WPA-Personal]
◆ **Wireless MAC Clone**	Wireless MAC Cloneを有効にすると、本製品のMACアドレスをクライアントのMACアドレスに変更することができます。 1. [Enable]（有効）にチェックをいれると設定が有効になります。 2. [Enable]（有効）にチェックをいれた場合、[MAC Source]を[Auto]（自動）または[Manual]（手動）に設定します。 3. [MAC Source]を[Manual]（手動）にした場合は、[MAC Address]欄にMACアドレスを入力するか、[Scan]をクリックして検索したMACアドレスを選択します。

メモ

[Authentication](認証方式)の設定内容は、選択した方式によって異なります。
詳細は『Authentication（認証）の設定について：p.30 』を参照してください。

■Authentication（認証）の設定について

[Wireless Setteing]画面では、認証方式として以下を選択できます。

◆ **Open Syetem**
オープンシステム認証を行います。ネットワーク側での認証を行いません。
設定方法については、『[Open System] または[Shared Key]を選択した場合：p.30 』を参照してください。

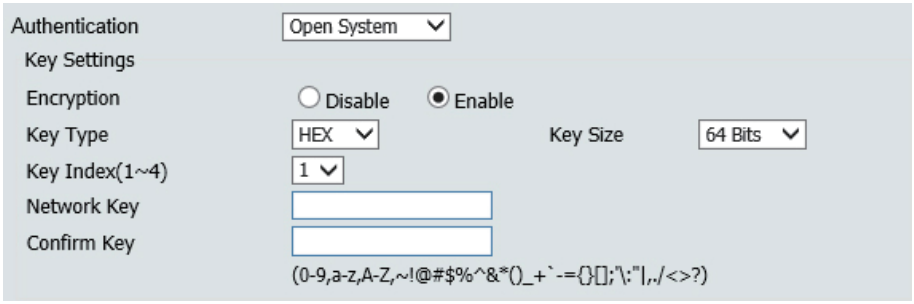
◆ **Shared Key**
同じWEP設定を行ったデバイス同士の通信のみ可能になります。
マルチSSIDが有効な場合は、本オプションは利用できません。
設定方法については、『[Open System] または[Shared Key]を選択した場合：p.30 』を参照してください。

◆ **WPA-Personal**
パスワードと認証キーの自動変更機能でセキュリティを提供します。RADIUS サーバは必要ありません。
設定方法については、『[WPA-Personal]を選択した場合：p.31 』を参照してください。

◆ **WPA-Enterprise**
ネットワーク内にRADIUS サーバがある場合に選択します。
設定方法については、『[WPA-Enterprise]を選択した場合：p.32 』を参照してください。

◆ **802.1X**
802.1X ネットワーク認証がある場合に選択します。
設定方法については、『[802.1 X]を選択した場合：p.33 』を参照

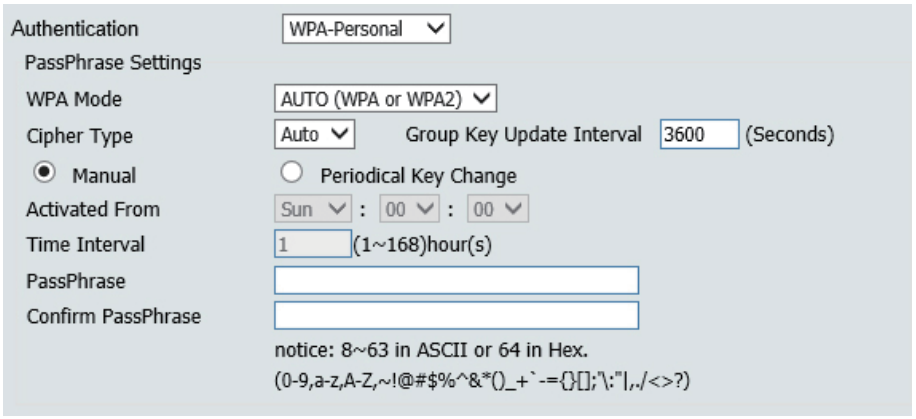
● [Open System] または[Shared Key]を選択した場合



◆ **Encryption**	暗号化を有効または無効にします。 ・選択肢：[Enable]（有効）[Disabled]（無効）
◆ **Key Type**	キーのタイプを選択します。 ・選択肢： - [HEX]（16 進数）：0 ～ 9、A ～ F までの半角英数字のキーを使用します。 - [ASCII]（半角英数字）：半角英数字のキーを使用します。
◆ **Key Size**	キーのサイズを選択します。 ・選択肢：[64 Bits] [128 Bits]
◆ **Key Index**	有効にするキーを選択します。 ・選択肢：[1] [2][3][4]
◆ **Network Key**	キーを入力します。
◆ **Confirm Key**	確認のため、再度キーを入力します。

● [WPA-Personal]を選択した場合

以下の画面でパスフレーズの設定を行います。

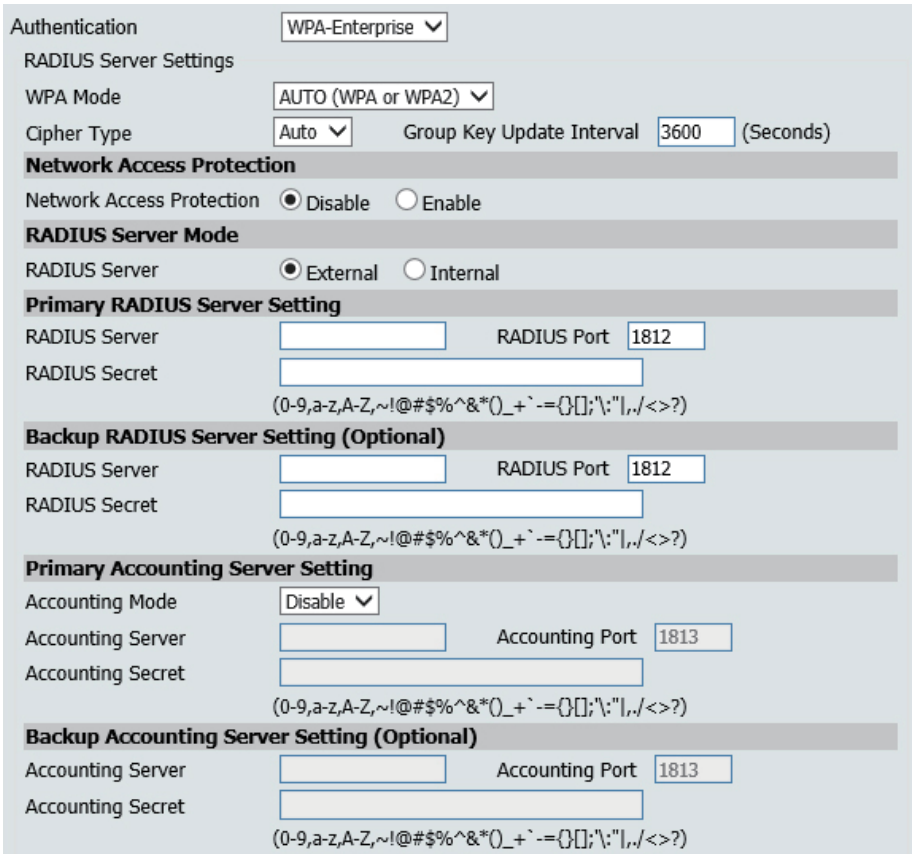


◆ **WPA Mode**	WPAのモードを選択します。 ・選択肢：[AUTO（WPA or WPA2）][WPA2 Only][WPA Only] WPA とWPA2 は異なるアルゴリズムを使用しています。 [AUTO（WPA or WPA2）]を指定するとWPA とWPA2 の両方を使用できます。
◆ **Cipher Type**	暗号化タイプを選択します。 ・選択肢：[Auto][AES][TKIP]
◆ **Group Key Update Interval**	グループキーを更新する間隔を設定します。 ・推奨値：1800（秒）
◆ **Manual**	パスフレーズを手動で設定するようにします。 [Manual] を選択した場合、使用するパスフレーズを入力します。
◆ **Periodical Key Change**	アクセスポイントが自動的にパスフレーズを変更するようにします。 [Periodical Key Change] を選択した場合、変更を行う周期を設定します。
◆ **Activated From**	[Periodical Key Change] を選択した場合、パスフレーズを変更する日時を設定します。
◆ **Time Interval**	[Periodical Key Change] を選択した場合、パスフレーズを変更する間隔を設定します。
◆ **PassPhrase**	[Manual] を選択した場合、パスフレーズを入力します。
◆ **Confirm PassPhrase**	[Manual] を選択した場合、確認のため再度パスフレーズを入力します。

メモ

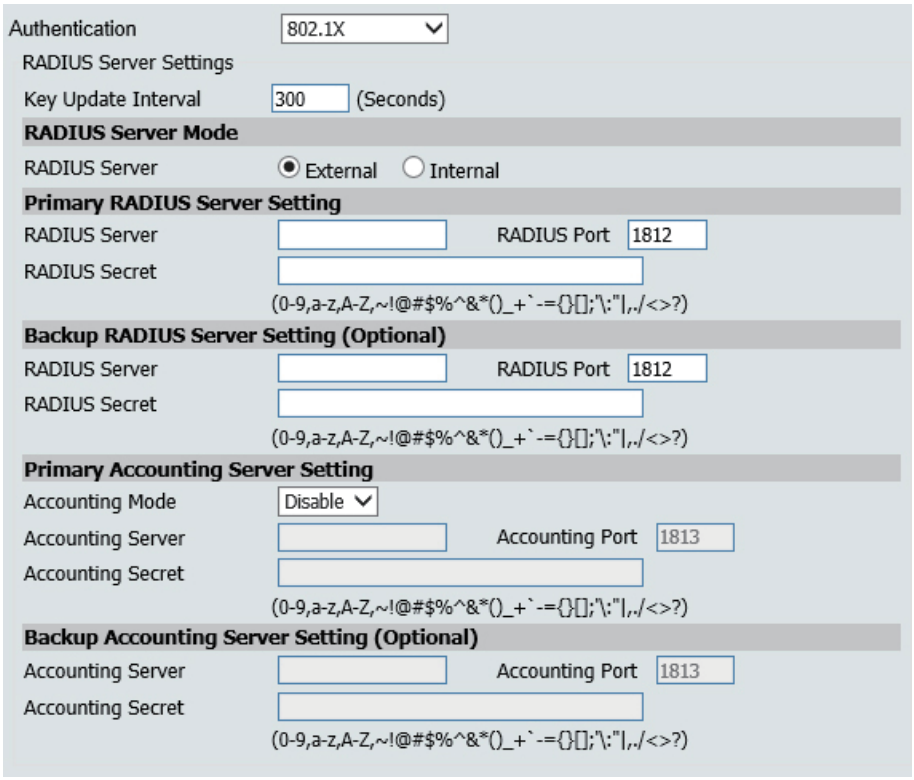
以下の項目は、アクセスポイントの通信モードをAccess Point モードに設定した場合のみ表示されます。
・[Manual] [Periodical Key Change][Activated From][Time Interval]

● [WPA-Enterprise]を選択した場合



◆ **WPA Mode**	WPAのモードを選択します。 ・選択肢：[AUTO（WPA or WPA2）][WPA2 Only][WPA Only] WPA とWPA2 は異なるアルゴリズムを使用しています。 [AUTO（WPA or WPA2）]を指定するとWPA とWPA2 の両方を使用できます。
◆ **Cipher Type**	暗号化タイプを選択します。 ・選択肢：[Auto][AES][TKIP]
◆ **Group Key Update Interval**	グループキーを更新する間隔を設定します。 ・推奨値：1800（秒）
◆ **Network Access Protection**	Microsoft Network Access Protectionを有効または無効にします。 ・選択肢：[Enable]（有効）[Disable]（無効）
◆ **Radius Server Mode**	RADIUSサーバのモードを選択します。 ・選択肢：[External]（外部）[Internal]（内部）
◆ **Primary Radius Server Settings**	プライマリRADIUSサーバの設定を行います。 ・**RADIUS Server:** RADIUS サーバのIP アドレスを入力します。 ・**RADIUS Port:** RADIUS サーバの認証に使用するポート番号を入力します。 初期値：[1812] ・**RADIUS Secret:** RADIUS シークレット（パスワード）を入力します。
◆ **Backup Radius Server Settings (Optional)**	バックアップRADIUSサーバの設定を行います。 ・**RADIUS Server:** RADIUS サーバのIP アドレスを入力します。 ・**RADIUS Port:** RADIUS サーバの認証に使用するポート番号を入力します。 初期値：[1812] ・**[RADIUS Secret:** RADIUS シークレット（パスワード）を入力します。
◆ **Primary Accounting Server Settings**	プライマリアカウンティングサーバの設定を行います。 ・**Accounting Mode:** アカウンティングモードを[Enable]（有効）[Disable]（無効）にします。 ・**Accounting Server:** アカウンティングサーバのIPアドレスを入力します。 ・**Accounting Port:** アカウンティングサーバの認証に使用するポート番号を入力します。 初期値：[1813] ・**Accounting Secret:** アカウンティングシークレット（パスワード）を入力します。
◆ **Backup Accounting Server Settings (Optional)**	バックアップアカウンティングサーバの設定を行います。 ・**Accounting Server:** アカウンティングサーバのIPアドレスを入力します。 ・**Accounting Port:** アカウンティングサーバの認証に使用するポート番号を入力します。 初期値：[1813] ・**Accounting Secret:** アカウンティングシークレット（パスワード）を入力します。

● [802.1 X]を選択した場合

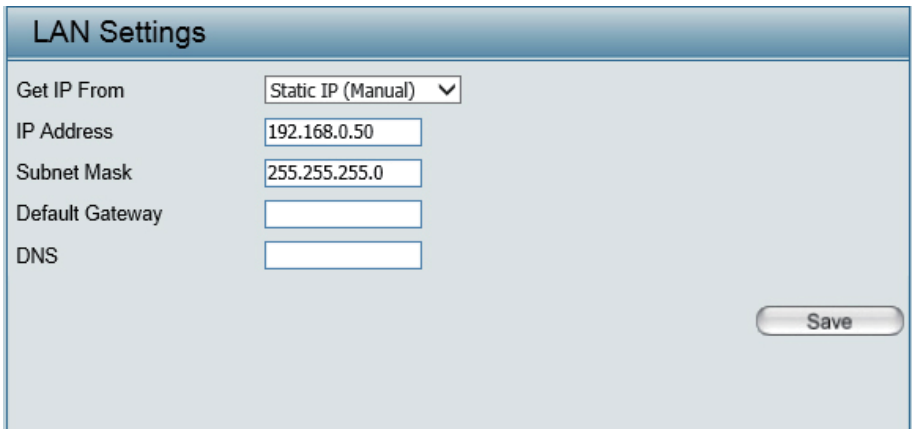


◆ **Key Update Interval**	キーを更新する間隔を設定します。 ・推奨値：300 (秒)
◆ **Radius Server Mode**	RADIUSサーバのモードを選択します。 ・選択肢：[External] (外部) [Internal] (内部)
◆ **Primary Radius Server Settings**	プライマリRADIUSサーバの設定を行います。 ・**RADIUS Server:** RADIUS サーバのIP アドレスを入力します。 ・**RADIUS Port:** RADIUS サーバの認証に使用するポート番号を入力します。 初期値：[1812] ・**RADIUS Secret:** RADIUS シークレット (パスワード) を入力します。
◆ **Backup Radius Server Settings (Optional)**	バックアップRADIUSサーバの設定を行います。 ・**RADIUS Server:** RADIUS サーバのIP アドレスを入力します。 ・**RADIUS Port:** RADIUS サーバの認証に使用するポート番号を入力します。 初期値：[1812] ・**RADIUS Secret:** RADIUS シークレット (パスワード) を入力します。
◆ **Primary Accounting Server Settings**	プライマリアカウンティングサーバの設定を行います。 ・**Accounting Mode:** アカウンティングモードを[Enable] (有効) [Disable] (無効) にします。 ・**Accounting Server:** アカウンティングサーバのIPアドレスを入力します。 ・**Accounting Port:** アカウンティングサーバの認証に使用するポート番号を入力します。 初期値：[1813] ・**Accounting Secret:** アカウンティングシークレット (パスワード) を入力します。
◆ **Backup Accounting Server Settings (Optional)**	バックアップアカウンティングサーバの設定を行います。 ・**Accounting Server:** アカウンティングサーバのIPアドレスを入力します。 ・**Accounting Port:** アカウンティングサーバの認証に使用するポート番号を入力します。 初期値：[1813] ・**Accounting Secret:** アカウンティングシークレット (パスワード) を入力します。

LAN Settings（LAN設定）

本製品のLAN インタフェースのIP 設定を行います。LAN IP アドレスは必要に応じて変更することも可能です。
LAN IP アドレスはネットワーク内部で使用されます。インターネット上には公開されません。

1. [Basic Settings] > [LAN] を選択します。
2. 以下の画面で設定を行います。



◆ **Get IP From**	IPアドレスの取得方法を選択します。 • [Static IP (Manual)]: 固定のIPアドレスを手動で設定します。 • [Dynamic (DHCP)]: DHCPサーバを使用してIPアドレスを設定します。 本製品のIPアドレスは、DHCPサーバから自動的に取得されます。[Dynamic (DHCP)]を選択した場合、その他の項目の設定は不要です。
◆ **IP Address**	IPアドレスを入力します。 • 初期値: 192.168.0.50
◆ **Subnet Mask**	サブネットマスクを入力します。 • 初期値: 255.255.255.0
◆ **Default Gateway**	デフォルトゲートウェイのIP アドレスを入力します。
◆ **DNS**	DNSのIPアドレスを入力します。

3. [Save] をクリックして設定を保存します。

IPv6 Settings（IPv6設定）

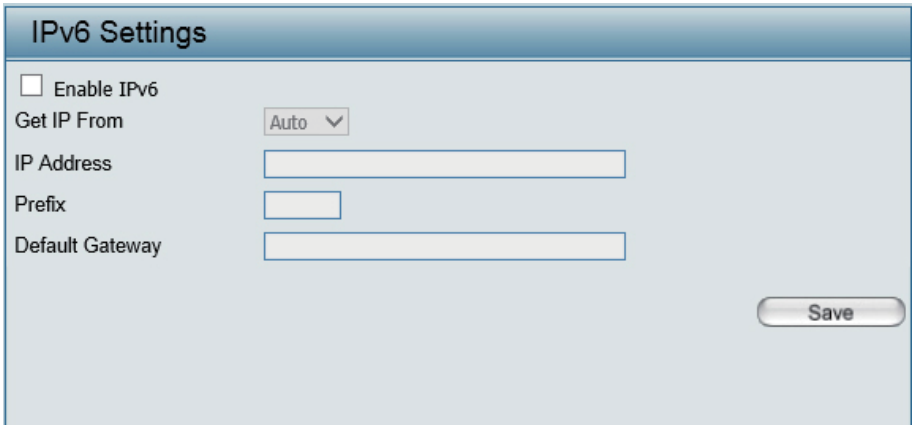
LAN インタフェースのIPv6 設定を行います。
本機能を有効にすると、IPv6 アドレスを使用してDAP-2660 にアクセスすることが可能となります。

メモ

IPv6設定を有効にした場合、AP Array機能は使用できません。

1. [Basic Settings] > [IPv6] を選択します。

2. 以下の画面で設定を行います。



◆ **Enable IPv6**	チェックをいれると、IPv6アドレスが有効になります。
◆ **Get IP From**	IPv6アドレスの取得方法を選択します。 ・[Static]: 固定のIPv6アドレスを手動で設定します。 ・[Auto]: 本製品のIPv6アドレスは、自動的に取得されます。[Auto]を選択した場合、その他の項目の設定は不要です。
◆ **IP Address**	IPv6アドレスを入力します。
◆ **Prefix**	プレフィックス長の値を入力します。
◆ **Default Gateway**	デフォルトゲートウェイのIP アドレスを入力します。

3. [Save] をクリックして設定を保存します。

Advanced Settings（詳細設定）

5

マルチSSIDやVLAN、キャプティブポータルなど、アクセスポイントの詳細設定を行います。

■ Advanced Settings について 37

■ Performance Settings（パフォーマンス設定） 37

■ Wireless Resource Control（ワイヤレスリソースコントロール） 39

■ Multi-SSID Settings（マルチSSID設定） 40

■ VLAN Settings（VLAN設定） 41

VLAN List タブ 41

Port List タブ 42

Add/Edit VLAN タブ 43

PVID Settingタブ 44

■ Wireless Intrusion Protection（不正AP検知） 45

■ Wireless Schedule Settings（スケジュール設定） 46

■ Internal RADIUS Server（RADIUSサーバ） 47

■ ARP Spoofing Prevention Settings（ARPスプーフィング防止設定） 48

■ Bandwidth Optimization（帯域幅最適化） 49

■ AP Array（APアレイ） 51

APアレイ構成図と設定手順 51

AP Array Scan (APアレイスキャン) 52

AP Array Configuration（APアレイ設定） 53

Auto-RF（自動RF） 54

Load Balance（ロードバランス） 54

■ Captive Portal（キャプティブポータル） 55

Captive Portal Authentication（キャプティブポータル認証） 55

暗号化タイプを[Passcode]にした場合 56

暗号化タイプを[Username/Password]にした場合 57

暗号化タイプを[Remote RADIUS]にした場合 58

暗号化タイプを[LDAP]にした場合 58

暗号化タイプを[POP3]にした場合 59

Login Page Upload（ログイン画面アップロード） 60

Web Redirection（Webリダイレクション） 60

MAC Bypass Settings（MAC Bypass 設定） 61

■ DHCP Server（DHCPサーバ設定） 62

Dynamic Pool Settings（ダイナミックプール設定） 62

Static Pool Settings（スタティックプール設定） 63

Current IP Mapping List（IPマッピングリスト） 64

■ Filters（フィルタ） 65

Wireless MAC ACL Settings（ワイヤレスMAC ACL） 65

WLAN Partition（WLANパーティション） 66

■ Traffic Control（トラフィックコントロール） 67

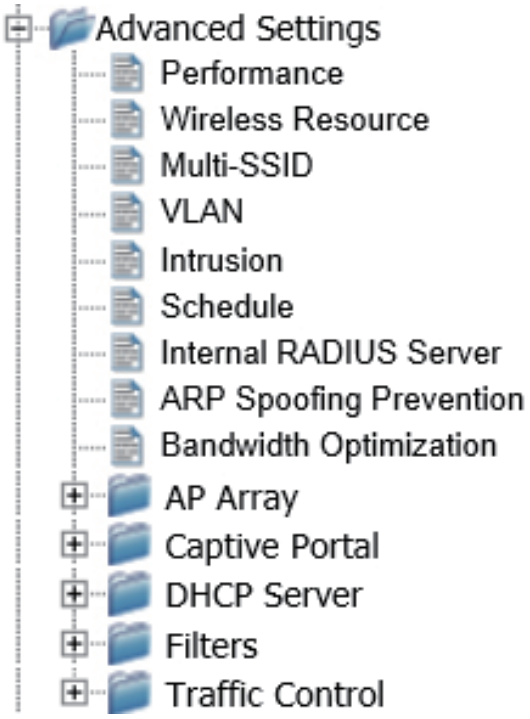
Uplink and Downlink Setting（アップリンク／ダウンリンク設定） 67

QoS（QoS設定） 68

Traffic Manager（トラフィックマネージャ） 69

Advanced Settings について

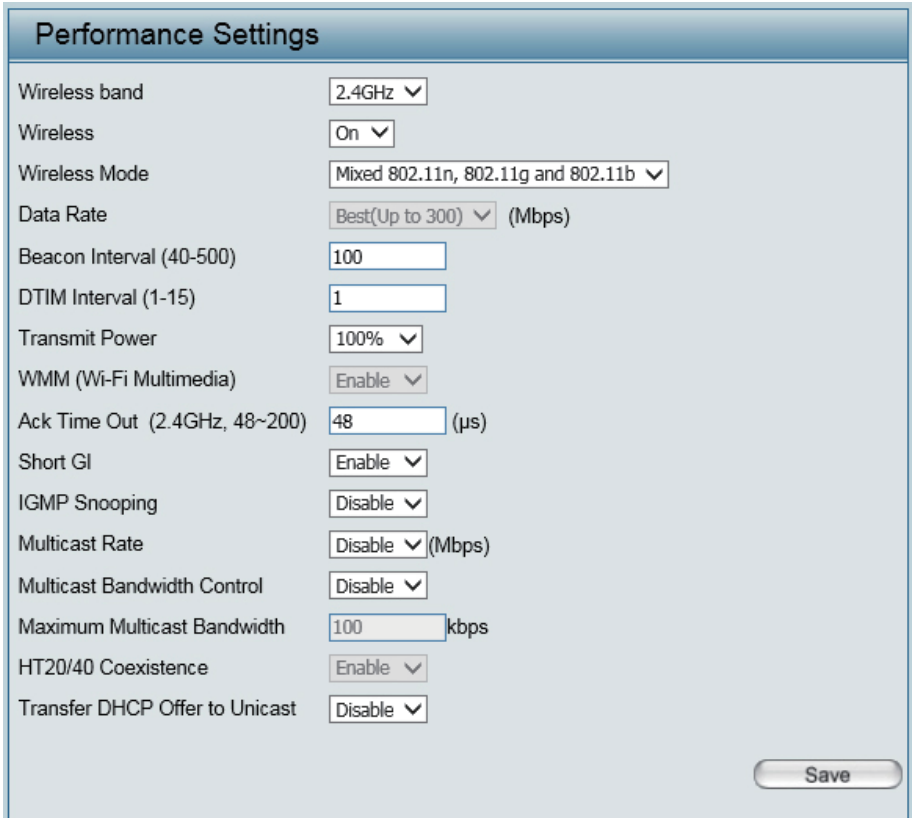
マルチSSIDやVLAN、キャプティブポータルなど、アクセスポイントの詳細設定を行います。



Performance Settings（パフォーマンス設定）

無線のパフォーマンス設定を行います。

1. [Advanced Settings] > [Performance] を選択します。
2. 以下の画面で設定を行います。



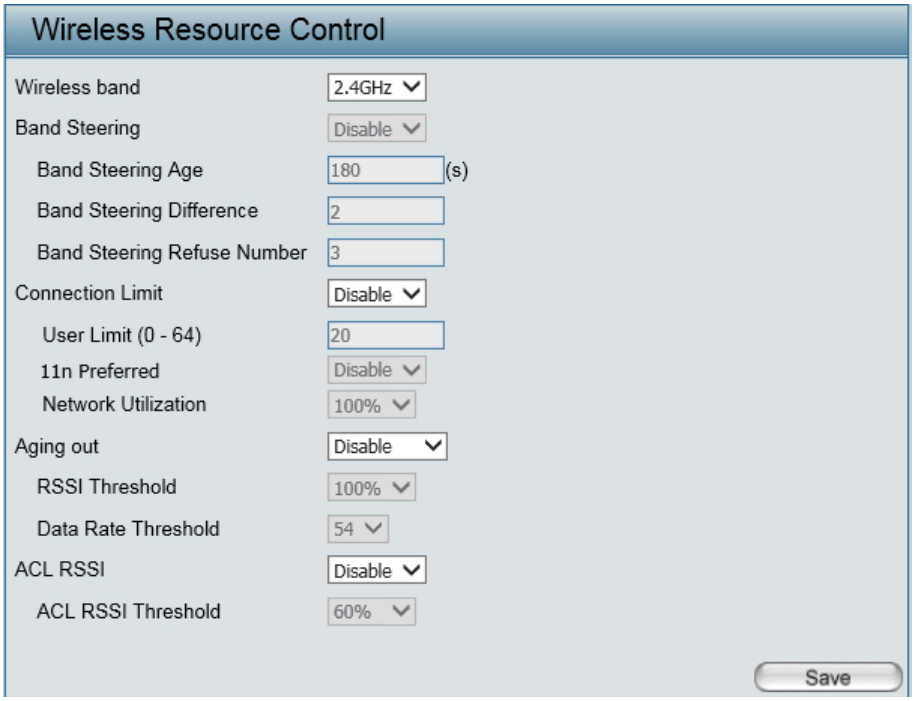
◆ **Wireless Band**	周波数帯を[2.4GHz]または[5GHz]から選択します。
◆ **Wireless**	無線機能を[On]または[Off]に選択します。 ・選択肢: [On]または[Off]
◆ **Wireless Mode**	ワイヤレスモードを選択します。選択肢は設定した周波数帯によって異なります。 ・選択肢([2.4GHz]を選択した場合): [Mixed 802.11n, 802.11g and 802.11b][Mixed 802.11g and 802.11b][802.11n Only] ・選択肢([5GHz]を選択した場合): [Mixed 802.11n, 802.11a][802.11a Only][802.11n Only] [Mixed 802.11ac] レガシークライアント (802.11g/b) 向けに互換性がある場合は、802.11n 規格の無線性能は低下します。
◆ **Data Rate**	ワイヤレスアダプタのベース転送速度を設定します。 ・選択肢([2.4GHz]を選択した場合): Best (Up to 54), 54, 48, 36, 24, 18, 12, 9, 6, 11, 5.5, 2,1 ・選択肢([5GHz]を選択した場合): Best (Up to 54), 54, 48, 36, 24, 18, 12, 9, 6 • 本製品のベース転送速度は接続しているデバイスのベース転送速度に左右されます。 • 障害物や干渉がある場合、転送速度は低下します。 • 本項目は、[Wireless Mode]で [802.11a Only][Mixed 802.11g and 802.11b]を選択した場合のみ設定できます。
◆ **Beacon Interval (40-500)**	ビーコンを送信する間隔を設定します。(単位:ミリ秒) ・初期値: 100 (※本値を推奨します) ・設定可能範囲:40-500 ビーコンとはアクセスポイントがネットワークと同期するために送信するパケットです。
◆ **DTIM Interval (1-15)**	DTIM (Delivery Traffic Indication Message) の間隔を設定します。 ・初期値: 1 ・設定可能範囲:1-15 DTIM とは、省電力モードの無線クライアントに対して、パケットが送信待ちであることを伝えるメッセージです。
◆ **Transmit Power**	無線の送信電力を設定します。 ・選択肢: 100%、50%、25%、12.5% 送信電力を調整することで、2 つのアクセスポイント間の干渉による無線適用範囲の重複を削減することができます。 例:無線適用範囲がエリアの半分をカバーしている場合は、50% を選択します。
◆ **WMM (Wi-Fi Multimedia)**	WMM (Wi-Fi Multimedia) を有効または無効にします。 ・選択肢:[Enable] (有効) [Disable] (無効) 本機能を「Enable」(有効) にするとWi-Fiネットワークを使用して快適にオーディオやビデオアプリケーションを利用できるようになります。
◆ **Ack Time Out (2.4GHz, 48~200)/ (5GHz, 25~200)**	「Acknowledgement Time Out」の値を入力します。 設定可能範囲は設定した周波数帯によって異なります。 ・設定可能範囲([2.4GHz]を選択した場合):48-200μs ・設定可能範囲([5GHz]を選択した場合):25-200μs 本項目を設定することで、効率的に長距離のスループットを最適化します。
◆ **Short GI**	Short GI(ショートガードインターバル)を有効または無効にします。 ・選択肢:[Enable] (有効) [Disable] (無効) ショートガードインターバルを有効にすると、スループットが増加します。同時に無線周波数の感度が上がるため、設置のエラー率が増加する場合もありますので、ご注意ください。
◆ **IGMP Snooping**	IGMP (Internet Group Management Protocol) スヌーピングを有効または無効にします。 ・選択肢:[Enable] (有効) [Disable] (無効) IGMPスヌーピング機能を利用すると、アクセスポイントはルータとIGMP ホスト間で送信されるIGMP クエリとIGMP レポートを認識するようになります。本機能が有効な場合、アクセスポイントを通過したIGMP メッセージに基づき、ホストにマルチキャストパケットを送信します。
◆ **Multicast Rate**	マルチキャストレートの数値を設定、または無効([Disable])にします。
◆ **Multicast Bandwidth Control**	マルチキャスト帯域幅管理を有効または無効にします。 ・選択肢:[Enable] (有効) [Disable] (無効)
◆ **Maximum Multicast Bandwidth**	最大マルチキャスト帯域幅を設定します。 ・初期値:100 [Multicast Bandwidth Control]を有効にした場合のみ設定します。
◆ **HT20/40 Coexistence**	20/40MHz 通信の同時利用を有効または無効にします。 ・選択肢:[Enable] (有効) [Disable] (無効) [Basic Settings] > [Wireless] で[Channel Width]が[Auto 20/40MHz] の場合に使用できます。
◆ **Transfer DHCP Offer to Unicast**	ユニキャストへのDHCPオファーを有効または無効にします。 ・選択肢:[Enable] (有効) [Disable] (無効)

3. [Save] をクリックして設定を保存します。

Wireless Resource Control（ワイヤレスリソースコントロール）

ワイヤレス接続設定を行い、デバイスがより適したワイヤレス接続を検知できるようにします。

1. [Advanced Settings] > [Wireless Resource] を選択します。
2. 以下の画面で設定を行います。



◆ **Wireless band**	周波数帯を[2.4GHz]または[5GHz]から選択します。
◆ **Band Steering**	バンドステアリングの設定を行います。 本機能は周波数帯を[2.4GHz]に設定した場合は使用できません。 • Band Steering Age : 情報をアップデートする間隔（秒）を指定します。 • Band Steering Difference : 「5GHz帯域クライアント数」マイナス「2.4GHz帯域クライアント数」の数値を設定します。差分のクライアント数がこの値を超過した場合、5GHz帯域のクライアントは、強制的に2.4GHz帯域へ接続されます。 • Band Steering Refuse Number : 5GHz帯域へのクライアント接続数が本項目で設定した値を超過すると、バンドステアリング機能が無効になります。 バンドステアリングは、ワイヤレスクライアントが2.4GHzと5GHzの両方をサポートしている場合、2.4GHzのシグナルの強さが十分でないときに、クライアントを5GHzに誘導する機能です。
◆ **Connect Limit**	接続するユーザ数の制限を行うことができます。 • Connection Limit : 接続制限を[Enable]（有効）または[Disable]（無効）に設定します。 • User Limit (0-64) : 接続可能なユーザ数を0-64から指定します。 • 11n Preferred : [Enable]（有効）または[Disable]（無効）を選択します。 有効にすると、11nクライアントの接続が優先されます。 • Network Utilization : 最大ネットワーク使用率を100%、80%、60%、40%、20%、0%から選択します。
◆ **Aging out**	ワイヤレスクライアントを切断する基準を設定します。 • Aging out : エージングアウトを[RSSI][Data Rate]または[Disable]（無効）に設定します。 • RSSI Threshold : RSSIのしきい値を10%～100%間で指定します。 • Data Rate Threshold : データレートのしきい値を6、9、12、18、24、36、48、54から指定します。
◆ **ACL RSSI**	ACL RSSIを有効または無効にします。 • ACL RSSI : ACL RSSIを[Enable]（有効）または[Disable]（無効）に設定します。 • ACL RSSI Threshold : ACL RSSIのしきい値を10%～100%間で指定します。

3. [Save] をクリックして設定を保存します。

Multi-SSID Settings（マルチSSID設定）

マルチSSIDの設定を行います。

1. [Advanced Settings] > [Multi SSID] を選択します。
2. 以下の画面で設定を行います。

◆ **Enable Multi-SSID**	チェックをいれるとマルチSSIDが有効になります。
◆ **Enable Priority**	チェックをいれるとSSID の優先機能が有効になります。 有効にすると、画面下部[Priority]で0 から7 までの優先値をSSID に設定できます。
◆ **Wireless Settings**	マルチSSIDのワイヤレス設定を行います。 • Band : 周波数帯を[2.4GHz]または[5Hz]に設定します。 • Index : マルチSSIDを以下から選択します。 [Primary SSID][SSID 1][SSID 2][SSID 3][SSID 4][SSID 5][SSID 6][SSID 7] • SSID : SSID名を入力します。 • SSID Visibility : [Enable]（有効）または[Disable]（無効）に設定します。 有効にするとSSID がネットワーク上にブロードキャストされ、すべてのネットワークユーザから閲覧できるようになります。 • Security セキュリティを[Open System][WPA-Personal][WPA-Enterprise][802.1X]から選択します。 選択した設定によって、画面下部に詳細設定を行う項目が表示されます。 セキュリティの詳細設定については『Authentication（認証）の設定について：p.30 』を参照してください。 • Priority SSIDの優先値を「0」～「7」の間で設定します。 • WMM (Wi-Fi Multimedia) [Enable]（有効）または[Disable]（無効）に設定します。 • Captive Profile [Enable]（有効）または[Disable]（無効）に設定します。

3. [Add] をクリックして設定を保存します。

◎ 追加したSSIDを削除する場合：

1. [Delete]欄のアイコンをクリックします。

◎ 追加したSSIDを編集する場合：

1. [Index]欄のインデックス名をクリックします。
2. [Add]をクリックして設定を保存します。

VLAN Settings（VLAN設定）

本製品はVLAN をサポートしています。
VLAN は、名前、VID.Mgmt（TCP スタック）、LAN、プライマリ/ マルチSSID で作成され、WDS 接続は物理ポートとしてVLAN に割り当てることが可能です。
VLAN タグなしで本製品に送信されたパケットには、すべてPVID を持つVLAN タグが付けられます。

1. [Advanced Settings] > [VLAN] を選択します。
2. [VLAN Status] で、VLAN を [Enable]（有効）または [Disable]（無効）に設定します。

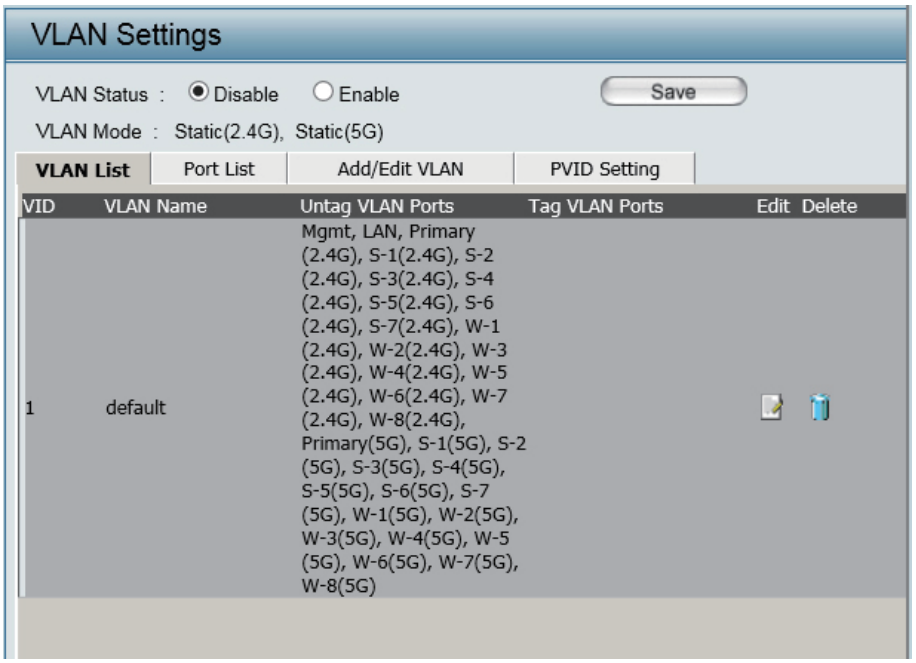
メモ

[VLAN Mode]には、現在のVLANモードが表示されます。

3. 以下のタブを使用して必要な設定を行います。
   - 『VLAN List タブ：p.41 』
   - 『Port List タブ：p.42 』
   - 『Add/Edit VLAN タブ：p.43 』
   - 『PVID Settingタブ：p.44 』

● VLAN List タブ

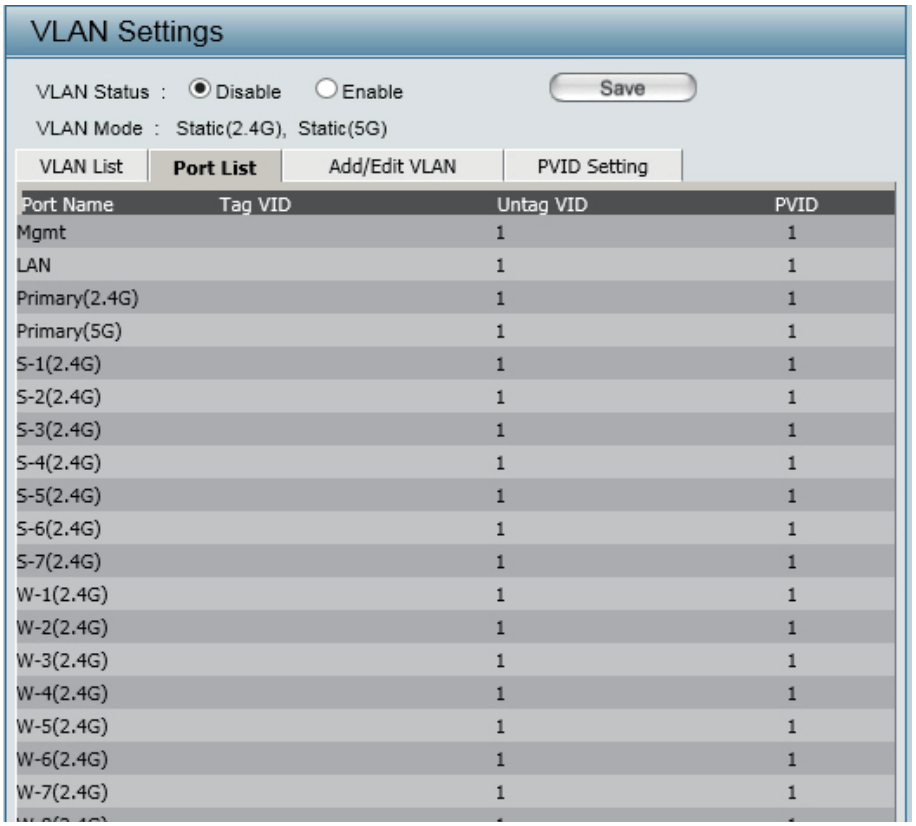
現在設定されているVLANのリストが表示されます。


VLAN Settings
VLAN Status : Disable Enable
Save
VLAN Mode : Static(2.4G), Static(5G)
VLAN List
Port List
Add/Edit VLAN
PVID Setting
VID
VLAN Name
Untag VLAN Ports
Tag VLAN Ports
Edit
Delete
1
default
Mgmt, LAN, Primary (2.4G), S-1(2.4G), S-2 (2.4G), S-3(2.4G), S-4 (2.4G), S-5(2.4G), S-6 (2.4G), S-7(2.4G), W-1 (2.4G), W-2(2.4G), W-3 (2.4G), W-4(2.4G), W-5 (2.4G), W-6(2.4G), W-7 (2.4G), W-8(2.4G), Primary(5G), S-1(5G), S-2 (5G), S-3(5G), S-4(5G), S-5(5G), S-6(5G), S-7 (5G), W-1(5G), W-2(5G), W-3(5G), W-4(5G), W-5 (5G), W-6(5G), W-7(5G), W-8(5G)

◆ **VID**	VLAN のIDが表示されます。
◆ **VLAN Name**	VLAN名が表示されます。
◆ **Untag VLAN Ports**	タグ無しVLANポートが表示されます。
◆ **Tag VLAN Ports**	タグ付きVLANポートが表示されます。
◆ **Edit**	アイコンをクリックすると[Add/Edit VLAN]タブの内容が表示され、VLANの編集を行うことができます。
◆ **Delete**	アイコンをクリックするとVLANを消去できます。

● Port List タブ

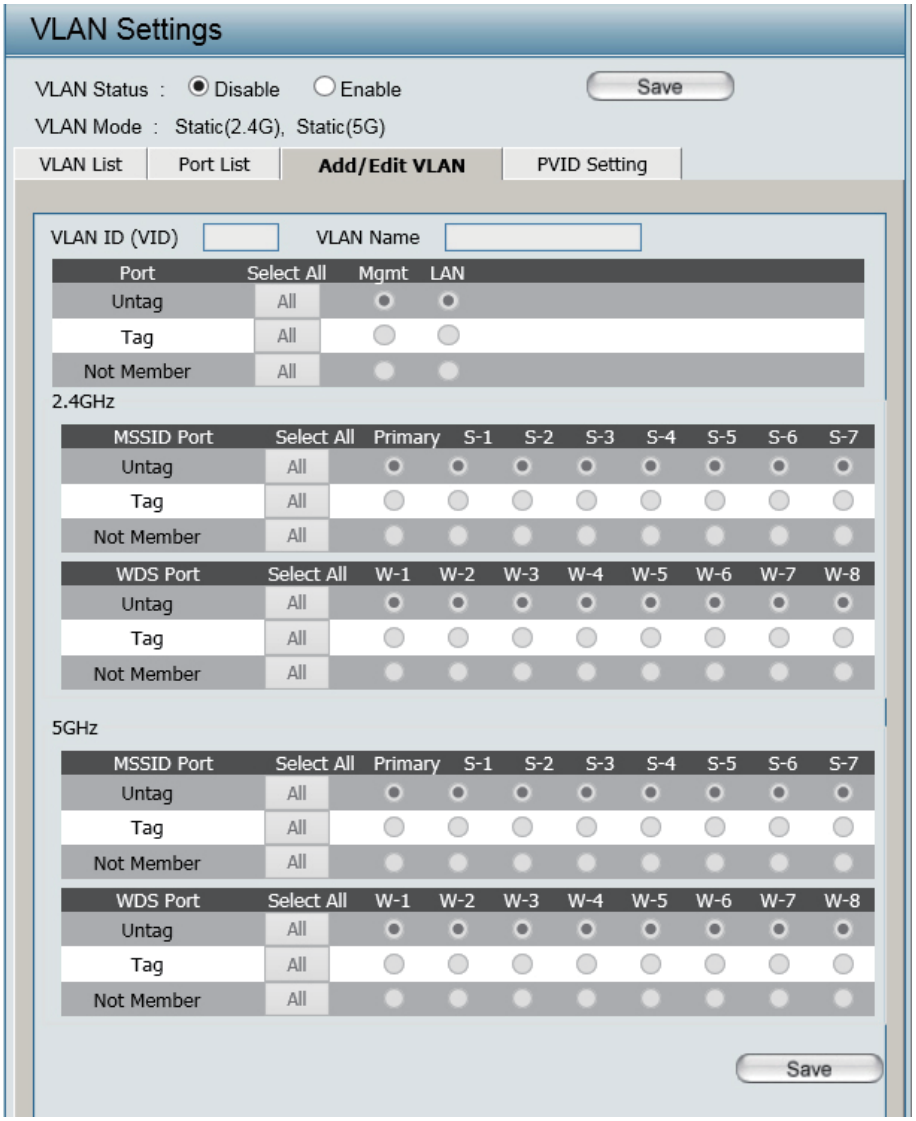
現在のポートのリストが表示されます。
VLAN にゲストネットワークと内部ネットワークを設定するためには、使用しているスイッチとDHCP サーバがVLAN をサポートしている必要があります。事前にスイッチのポートがIEEE 802.1Q 定義のVLAN タグ付きパケットをサポートするように設定を行ってください。



◆ **Port Name**	VLAN のIDが表示されます。
◆ **Tag VID**	VLAN名が表示されます。
◆ **Untag VID**	タグ無しVLANポートが表示されます。
◆ **PVID**	タグ付きVLANポートが表示されます。

● Add/Edit VLAN タブ

新しいVLANの追加または既存のVLANの編集を行います。



◆ **VLAN ID (VID)**	内部VLAN 用の番号を入力します。 ・設定可能範囲：1-4094
◆ **VLAN Name**	追加または変更するVLAN 名を入力します。
◆ **Port** ◆ **MSSID Port** ◆ **WDS Port**	• Untag - ポートをタグなしとして定義します。 • Tag - ポートをタグ付きとして定義します。 • Not Member - ポートをVLAN メンバとしないように定義します。 All を選択するとすべてのポートが選択されます。

◎ 新しいVLANを追加する場合：

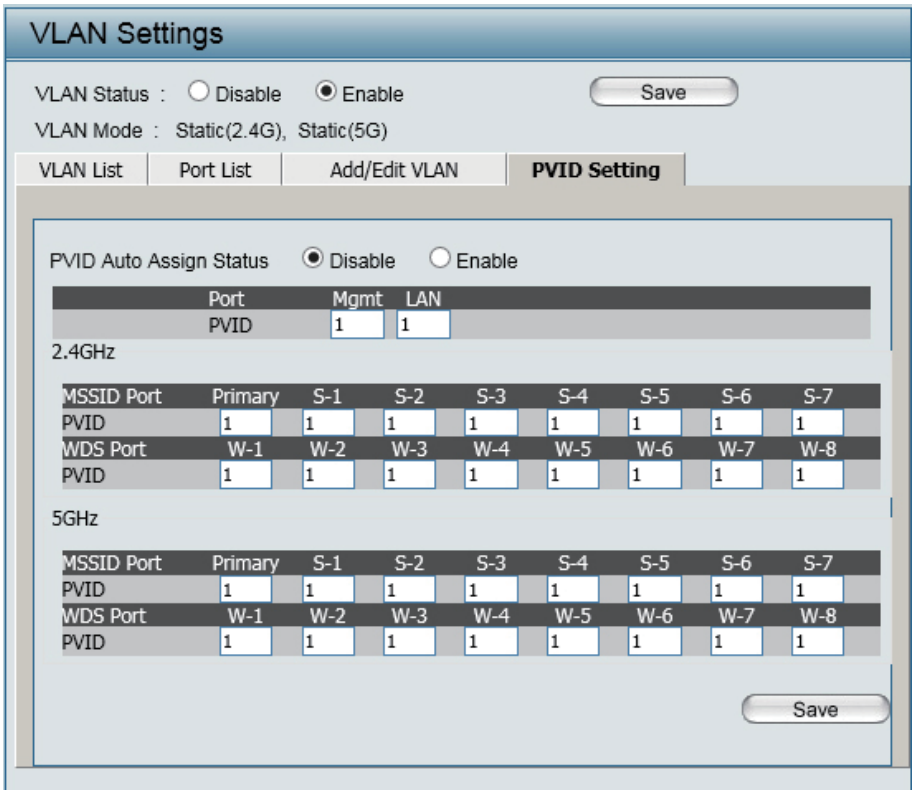
1. [VLAN Status]を[Enable]にします。
2. [VLAN ID（VID）]に識別番号、[VLAN Name]に識別名を入力します。
3. [Save]をクリックして設定を保存します。

◎ 既存のVLANを編集する場合：

1. [VLAN List]タブで編集するVLANの アイコンをクリックします。
2. [Add/Edit VLAN]タブが表示されるので、VLANの編集を行います。
3. [Save]をクリックして設定を保存します。

● PVID Settingタブ

PVID 自動割り当て設定および各PVID 設定を行います。


VLAN Settings
VLAN Status : Disable Enable
Save
VLAN Mode : Static(2.4G), Static(5G)
VLAN List
Port List
Add/Edit VLAN
PVID Setting
PVID Auto Assign Status Disable Enable
Port Mgmt LAN
PVID 1 1
2.4GHz
MSSID Port Primary S-1 S-2 S-3 S-4 S-5 S-6 S-7
PVID 1 1 1 1 1 1 1 1
WDS Port W-1 W-2 W-3 W-4 W-5 W-6 W-7 W-8
PVID 1 1 1 1 1 1 1 1
5GHz
MSSID Port Primary S-1 S-2 S-3 S-4 S-5 S-6 S-7
PVID 1 1 1 1 1 1 1 1
WDS Port W-1 W-2 W-3 W-4 W-5 W-6 W-7 W-8
PVID 1 1 1 1 1 1 1 1
Save

◆ **PVID Auto Assign Status**	PVID自動割り当て設定を有効または無効にします。 ・選択肢：[Enable]（有効）[Disable]（無効）
◆ **Port** ◆ **MSSID Port** ◆ **WDS Port**	PVID自動割り当て設定を有効または無効にした場合に、PVIDの設定を行います。

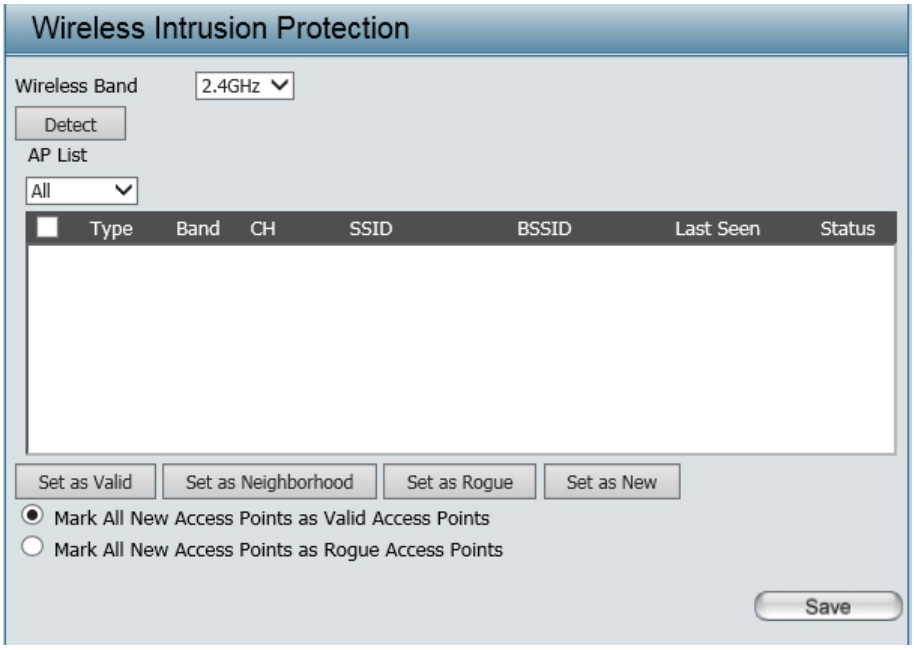
4. [Save] をクリックして設定を保存します。

Wireless Intrusion Protection（不正AP検知）

アクセスポイントの検知を行い、検知したアクセスポイントを分類することができます。

1. [Advanced Settings] > [Intrusion] を選択します。

2. 以下の画面でアクセスポイントの検知と分類を行います。



◆ **Wireless Band**	周波数帯を[2.4GHz]または[5GHz]から選択します。
◆ **Detect**	アクセスポイントの検知を実行します。
◆ **AP List**	検知したアクセスポイントのリストを表示します。 表示するアクセスポイントは以下から選択できます。 • [All] : すべてのアクセスポイント • [Valid] : 正しいアクセスポイント • [Neighbor] : 隣接したアクセスポイント • [Rogue] : 不正なアクセスポイント • [New] : 新しいアクセスポイント
◆ **Set as Valid**	チェックをいれたアクセスポイントを、正しいアクセスポイントとして分類します。
◆ **Set as Neighborhood**	チェックをいれたアクセスポイントを、隣接したアクセスポイントとして分類します。
◆ **Sert as Rogue**	チェックをいれたアクセスポイントを不正なアクセスポイントとして分類します。
◆ **Set as New**	チェックをいれたアクセスポイントを、正しいアクセスポイントとして分類します。

メモ

- [Mark All New Access Points as Valid Access Points]を選択すると、新に検知されたすべてのアクセスポイントが正しいアクセスポイントとして分類されます。
- [Mark All New Access Points as Rogue Access Points]を選択すると、新に検知されたすべてのアクセスポイントが不正なアクセスポイントとして分類されます。

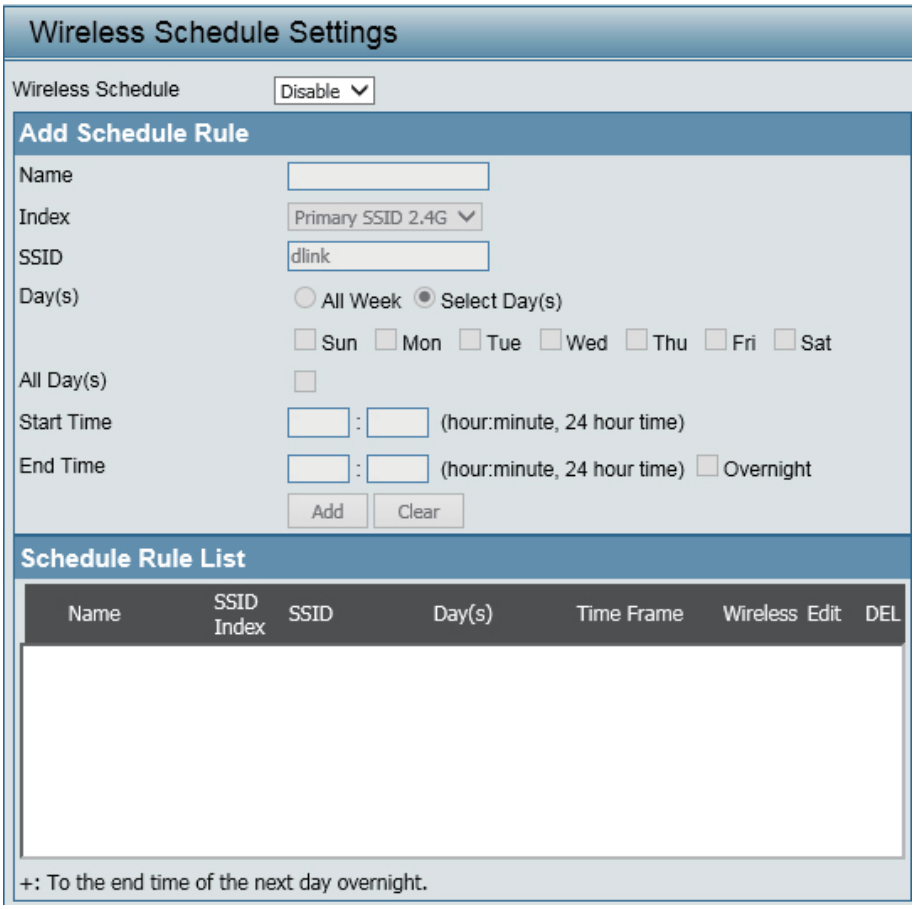
3. [Save] をクリックして設定を保存します。

Wireless Schedule Settings（スケジュール設定）

無線機能のスケジュールルールを追加または編集することができます。

1. [Advanced Settings] > [Schedule] を選択します。

2. 以下の画面で設定を行います。



◆ **Wireless Schedule**	無線スケジュール設定を有効または無効にします。 • 選択肢：[Enable]（有効）[Disable]（無効）
◆ **Add Schedule Rule**	スケジュールルールの追加・編集を行います。 • Name：ルール名を入力します。 • Index：ドロップダウンリストから対象のSSIDを選択します。 • SSID：ネットワーク名（SSID）が表示されます。 • Days：[All Week]（毎日）または[Select Day (s)]（曜日指定）を選択します。 [Select Day (s)]を選択した場合、ルールを適用する曜日を指定します。 • All Day(s): チェックすると終日が選択されます。 • Start Time/End Time： 開始時刻と終了時刻を指定します。 [Overnight]にチェックをいれると開始時刻から日付をこえた時刻を終了時刻に設定できます。時刻は24時間表示で指定してください。 • Add：設定した内容を追加します。 • Clear：設定した内容を取り消します。
◆ **Schedule Rule List**	設定したスケジュールルールが表示されます。

◎ スケジュールルールを削除する場合：

1. [Schedule Rule List]欄の アイコンをクリックします。

◎ スケジュールルールを編集する場合：

1. [Schedule Rule List]の アイコンをクリックします。
2. [Add Schedule Rule]でルールを編集します。
3. [Add]をクリックして設定を保存します

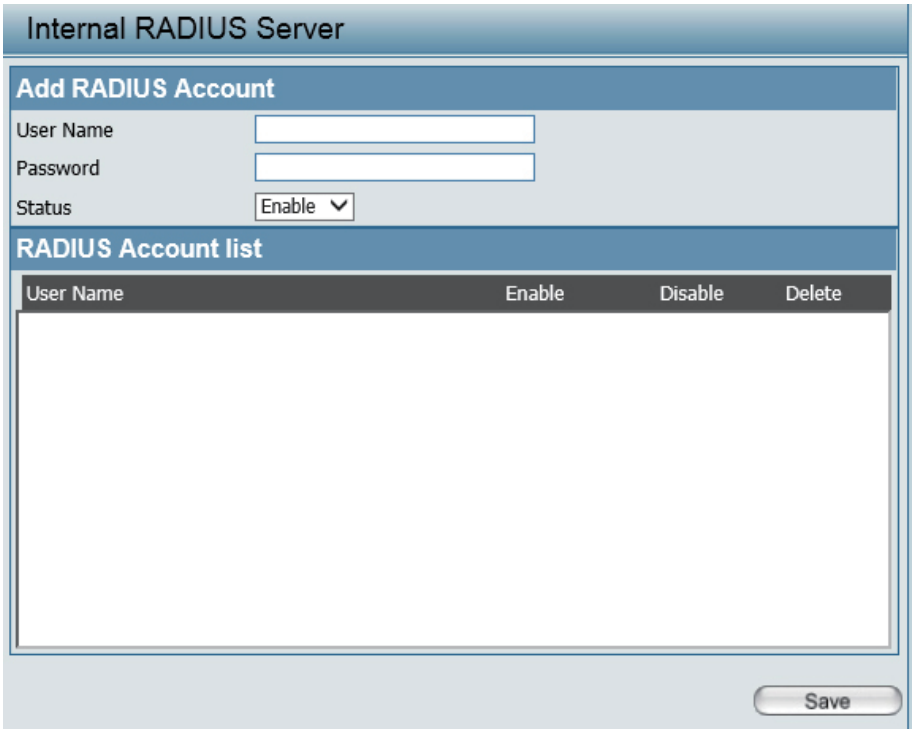
3. [Save] をクリックして設定を保存します。

Internal RADIUS Server（RADIUSサーバ）

本製品はRADIUSサーバを内蔵しています。
本項目では、RADIUSアカウントの作成／削除方法およびアカウントを有効／無効にする方法について説明します。
作成するアカウント数は30個以内にすることをおすすめします。

1. [Advanced Settings] > [Internal RADIUS Server] を選択します。

2. 以下の画面で設定を行います。



◆ **Add RADIUS Account**	RADIUSアカウントの追加を行います。 • User Name : アカウントのユーザ名を入力します。 • Password : 正しいアカウントのパスワードを入力します。パスワードの文字数は8～64以内に設定 • Status : アカウントのステータスを[Enable](有効)または[Disable](無効)にします。
◆ **RADIUS Account list**	作成したアカウントのリストが表示されます。 アカウントを削除する場合は、アイコンをクリックします。

3. [Save] をクリックして設定を保存します。

ARP Spoofing Prevention Settings （ARPスプーフィング防止設定）

ARP スプーフィング防止機能は、IP/MAC アドレスをマッピングすることにより、ARP スプーフィング攻撃を防止する機能です。

1. [Advanced Settings] > [ARP Spoofing Prevention] を選択します。

2. 以下の画面で設定を行います。

◆ **ARP Spoofing Prevention**	ARPスプーフィング防止を有効または無効にします。 • 選択肢：[Enable]（有効）[Disable]（無効）
◆ **Add Gateway Address**	ゲートウェイアドレスの追加・編集を行います。 • Gateway IP Address : アカウントのユーザ名を入力します。 • Gateway MAC Address : 正しいアカウントのパスワードを入力します。 • Add : 設定した内容を追加します。 • Clear : 設定した内容を取り消します。
◆ **Gateway Address List**	ゲートウェイアドレスのリストが表示されます。

◎ ゲートウェイアドレスを削除する場合：

1. [Gateway Address List]欄の🗑アイコンをクリックします。

◎ ゲートウェイアドレスを編集する場合：

1. [Gateway Address List]の📝アイコンをクリックします。
2. [Add Gateway Address]でルールを編集します。
3. [Add]をクリックして設定を保存します

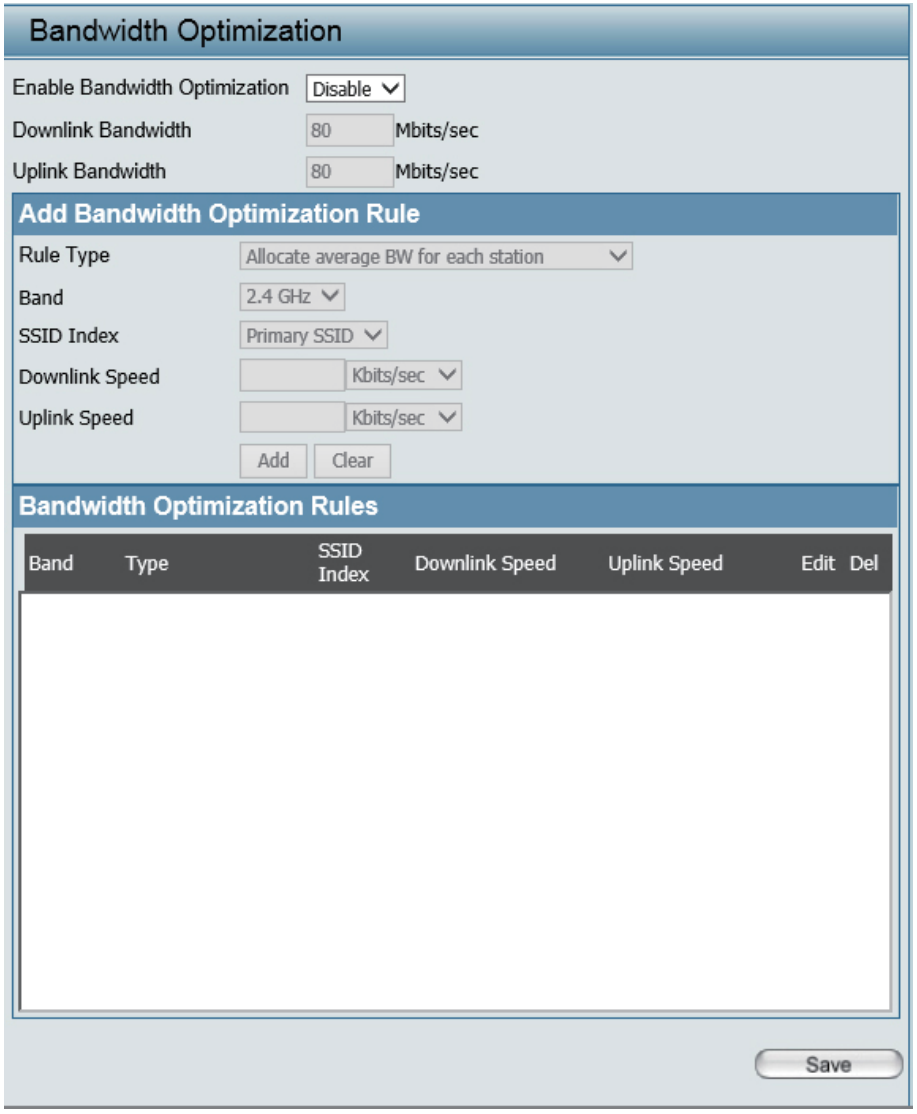
3. [Save] をクリックして設定を保存します。

Bandwidth Optimization（帯域幅最適化）

帯域幅最適化機能を使用すると、本製品およびワイヤレスクライアントの帯域幅を管理することができます。
本項目では、帯域幅最適化機能の設定方法について説明します。

1. [Advanced Settings] > [Bandwidth Optimization] を選択します。

2. 以下の画面で設定を行います。



◆ **Enable Bandwidth Optimization**	帯域幅最適化を有効または無効にします。 • 選択肢：[Enable]（有効）[Disable]（無効）
◆ **Downlink Bandwidh**	ダウンリンクの帯域幅を入力します。 単位：Mbits（秒）
◆ **Uplink Bandwidth**	アップリンクの帯域幅を入力します。 単位：Mbits（秒）
◆ **Add Bandwidth Optimization Rule**	帯域幅最適化ルールの追加・編集を行います。 • Rule Type : 以下からルールタイプを指定します。 - Allocate average BW for each station 各クライアントに平均の帯域を割り当てます。 - Allocate maximum BW for each station 各クライアントに最大の帯域を割り当てます。 - Allocate different BW for a/b/g/n stations a/b/g/nのクライアントに異なる帯域を割り当てます。 ・11b/g/nクライアント：10% / 20% / 70% ・11a/nクライアント：20% / 80% - Allocate specific BW for SSID すべてのクライアントで全体の帯域幅をシェアします。 • Band : 帯域幅を[2.4GHz]または[5GHz]から選択します。 • SSID Index : ドロップダウンリストから対象のSSIDを選択します。 • Downlink Speed : ダウンリンクの速度を設定します。単位はKbit（秒）またはMbits（秒）から選択できます。 • Uplink Speed : アップリンクの速度を設定します。単位はKbit（秒）またはMbits（秒）から選択できます。 • Add : 設定を追加します。 • Clear : 設定した内容を取り消します。
◆ **Bandwidth Optimization Rules**	作成したルールのリストが表示されます。

◎ 帯域幅最適化ルールを削除する場合：

1. [Bandwidth Optimization Rules]欄の🗑アイコンをクリックします。

◎ 帯域幅最適化ルールを編集する場合：

1. [Bandwidth Optimization Rules]の📝アイコンをクリックします。
2. [Add Bandwidth Optimization Rule]でルールを編集します。
3. [Add]をクリックして設定を保存します

3. [Save] をクリックして設定を保存します。

AP Array（APアレイ）

APアレイは、複数のアクセスポイントの管理をより簡単に行えるようにする機能です。
小規模オフィスの無線LAN管理に適しています。
複数のアクセスポイントを単一のグループに設定し、アクセスポイントの管理を簡素化することができます。

APアレイ機能を使用する場合、グループ内のアクセスポイントを以下のいずれかに設定します。

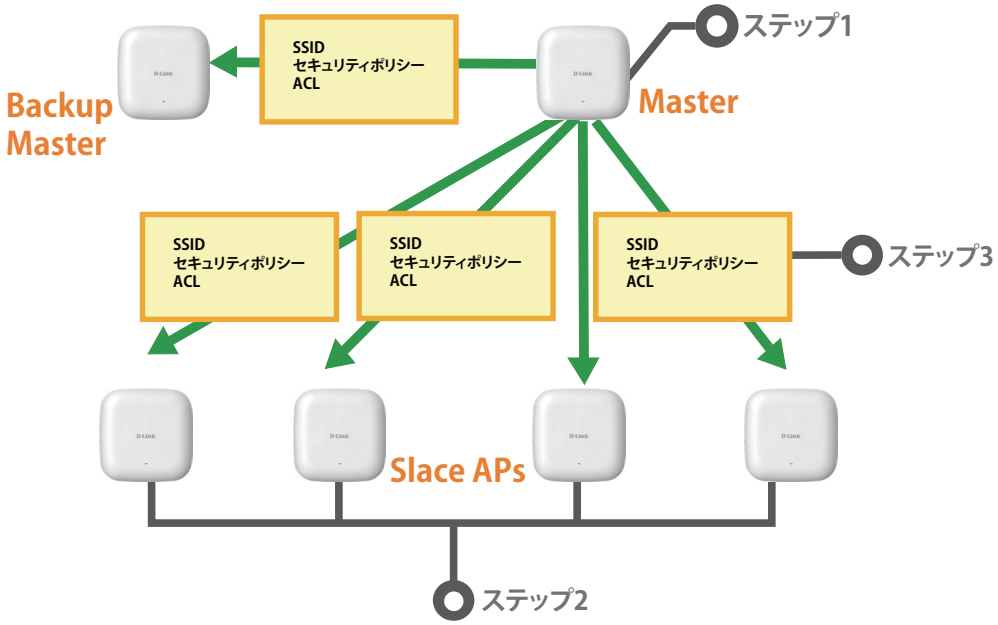
- Master
  アレイ内の全AP の設定を行うことができます。各アレイには 1 つのみ設定できます。
- Backup Master
  Master AP が停止してしまった場合、Backup Master AP が Master AP の機能を引き継ぎます。各アレイは最大2 つまでのBackup Master AP を設定することが可能です。
- Slave
  Master APの設定に従います。

メモ

- 最大32個のアクセスポイントを 1 つのグループに設定することができます。

■APアレイ構成図と設定手順

AP アレイの構成図の例と、設定手順の概要です。



◆ Step 1 -「Master AP」の配置:

1. AP を 1 つ「Master」として指定します。
2. AP Array ID と AP Array Password を設定します。
3. AP の設定をします。

◆ Step 2 -「Slave APs」の配置:

1. 「Slave APs」に「Master」のアレイ ID とパスワードを設定します。

◆ Step 3 - 設定の同期:

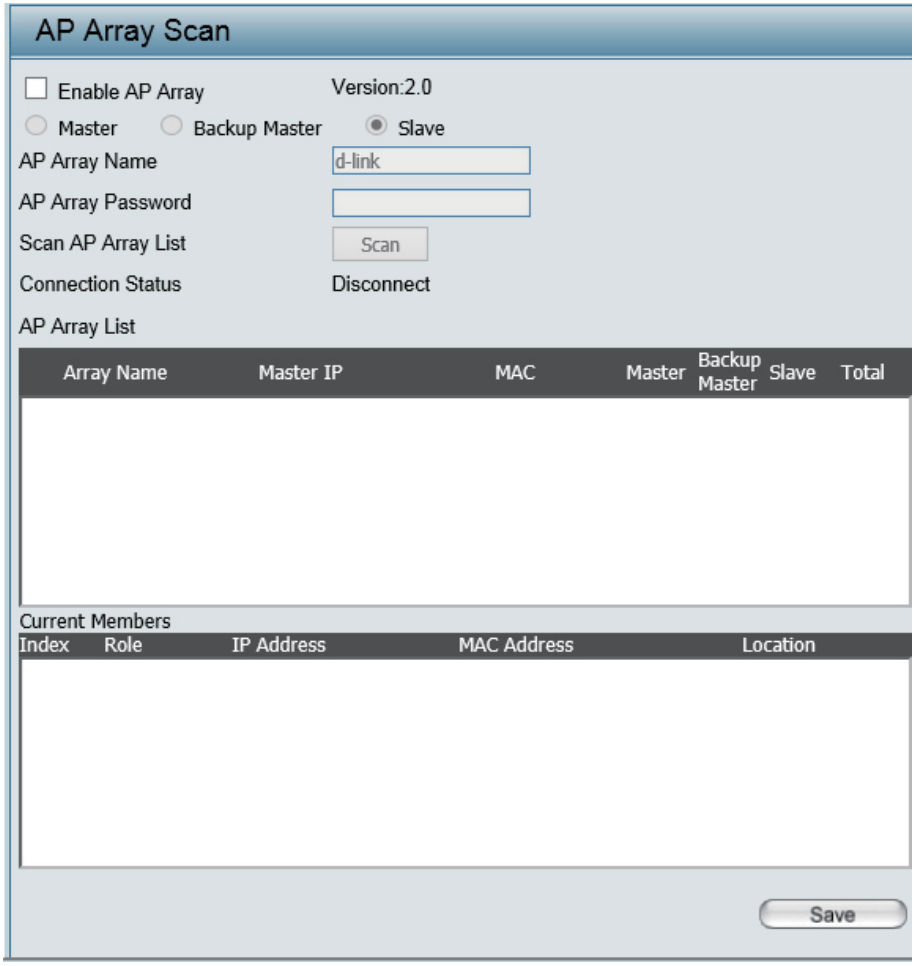
1. 「Backup Master」とすべての「Slave」AP が自動的に「Master」の設定に同期します。
   同期する設定項目を選択することも可能です。

■AP Array Scan (APアレイスキャン)

本項目では、APアレイ機能を有効にするほか、APアレイ名、パスワードの設定などを行います。
また、APアレイのリストが表示されます。

1. [Advanced Settings] > [AP Array] > [AP Array Scan] を選択します。

2. 以下の画面で設定を行います。



◆ **Enable AP Array**	チェックをいれるとAP アレイが有効になります。 有効にした場合は、以下からAPアレイの設定を選択します。 • Master アレイ内の全AP の設定を行うことができます。各アレイには 1 つのみ設定できます。 • Backup Master Master AP が停止してしまった場合、Backup Master AP が Master AP の機能を引き継ぎます。各アレイは最大2 つまでのBackup Master AP を設定することが可能です。 • Slave Master APの設定に従います。
◆ **AP Array Name**	APアレイの名称を入力します。
◆ **AP Array Password**	APアレイのパスワードを設定します。
◆ **Scan AP Array List**	ネットワーク上にあるアクセスポイントを検索します。
◆ **Connection Status**	現在の AP アレイの状態が表示されます。
◆ **AP Array List**	APアレイのリストが表示されます。
◆ **Current Members**	現在のAP アレイのメンバを表示します。

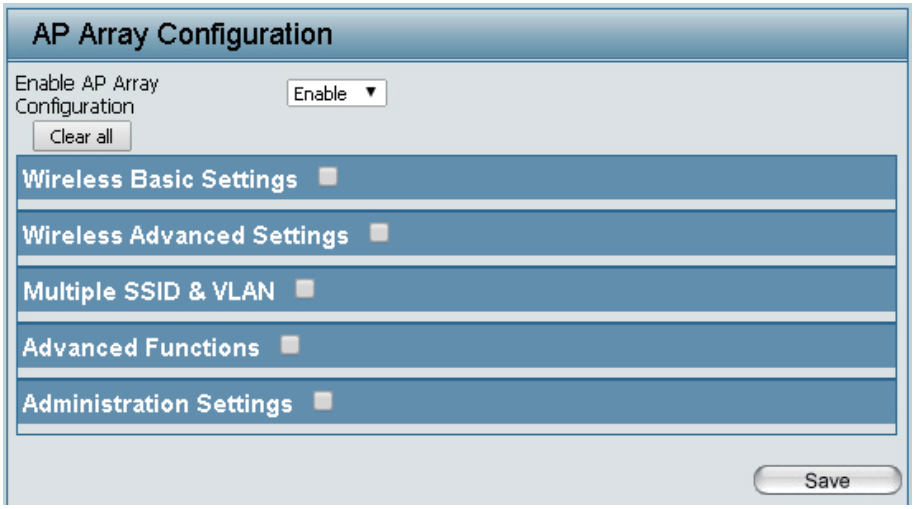
3. [Save] をクリックして設定を保存します。

■AP Array Configuration（APアレイ設定）

APアレイで同期を行う項目を選択します。

1. [Advanced Settings] > [AP Array] > [Configuration Settings] を選択します。

2. 以下の画面で設定を行います。



◆ **Enable AP Array Configuration**	APアレイ設定を有効または無効にします。 ・選択肢：[Enable]（有効）[Disable]（無効）
◆ **Clear all**	選択した項目をすべて取り消します。
◆ **Wireless Basic Settings**	以下から同期を行う項目を選択します。 • Network Name (SSID)　• SSID Visibility • Auto Channel Selection　• Channel Width • Security　• Captive Profile
◆ **Wireless Advanced Settings**	以下から同期を行う項目を選択します。 • Wireless　• Wireless Mode • Data Rate　• Beacon Interval • DTIM Interval　• Transmit Power • WMM (Wi-Fi Multimedia)　• Ack Time Out • Wireless ACL　• Short GI • Link Integrity　• Connection Limit • IGMP Snooping
◆ **Multiple SSID & VLAN**	以下から同期を行う項目を選択します。 • SSID　• SSID Visibility • Security　• WMM • Captive Profile　• VLAN
◆ **Advanced Functions**	以下から同期を行う項目を選択します。 • Schedule Settings　• QoS Settings • Log Settings　• Time and Date Settings • ARP Spoofing Prevention　• Bandwidth Optimization • Captive Portal　• Auto RF • Load Balance　• DHCP server Settings
◆ **Administration Settings**	以下から同期を行う項目を選択します。 • System Name Settings　• SNMP Settings • Login Settings　• Console Settings • Ping Control Setting

3. [Save] をクリックして設定を保存します。

■Auto-RF（自動RF）

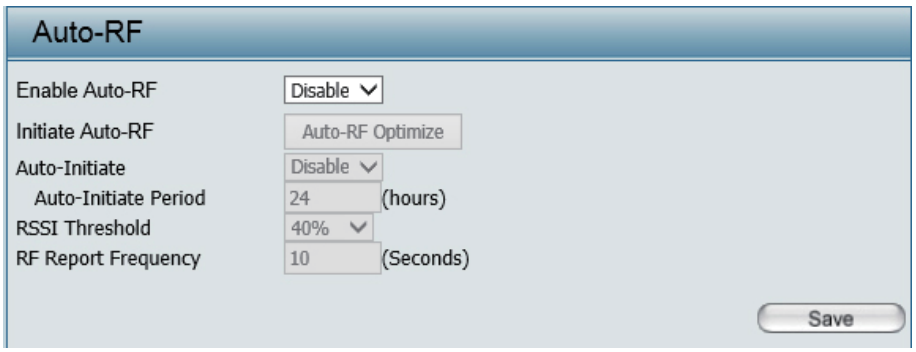
自動RFの有効・無効を選択します。
有効にした場合は、自動初期化の周期やRSSIしきい値などの設定を行います。

メモ

自動RFは、AP Array Scan(APアレイスキャン)画面でAPアレイの設定をSlaveにした場合は有効にできません。

1. [Advanced Settings] > [AP Array] > [Configuration Settings] を選択します。

2. 以下の画面で設定を行います。



◆ **Enable Auto-RF**	自動RFを有効または無効にします。 ・選択肢：[Enable]（有効）[Disable]（無効）
◆ **Initiate Auto-RF**	自動RFの初期化を行います
◆ **Auto-Initiate**	自動RFの自動初期化を有効または無効にします。 ・選択肢：[Enable]（有効）[Disable]（無効）
◆ **Auto-Initiate Period**	自動RFの自動初期化を有効にした場合、自動的に初期化を行う周期を指定します。（単位：時間） ・選択可能範囲：1-24（時間）
◆ **RSSI Threshold**	RSSIしきい値を選択します。 ・選択可能範囲：10-100（%）
◆ **RF Report Frequency**	RFリポートを行う頻度を入力します。（単位：秒）

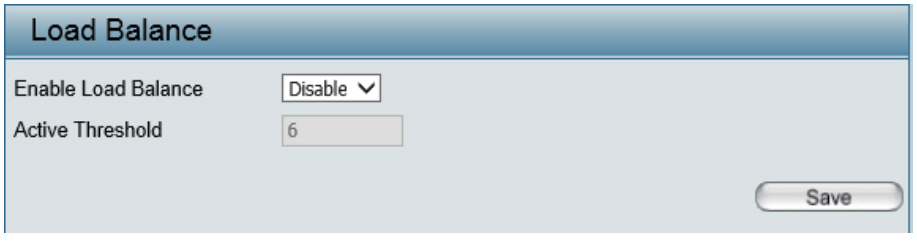
3. [Save] をクリックして設定を保存します。

■Load Balance（ロードバランス）

APアレイのロードバランスの有効・無効を選択します。有効にした場合はしきい値の設定を行います。

1. [Advanced Settings] > [AP Array] > [Load Balance] を選択します。

2. 以下の画面で設定を行います。



◆ **Enable Load Balance**	ロードバランスを有効または無効にします。 ・選択肢：[Enable]（有効）[Disable]（無効）
◆ **Active Threshold**	しきい値を入力します。

3. [Save] をクリックして設定を保存します。

Captive Portal（キャプティブポータル）

キャプティブポータルは、Web認証を行う機能です。
認証されていないクライアントがアクセスポイントに接続すると、Webブラウザによって認証画面へリダイレクトされます。

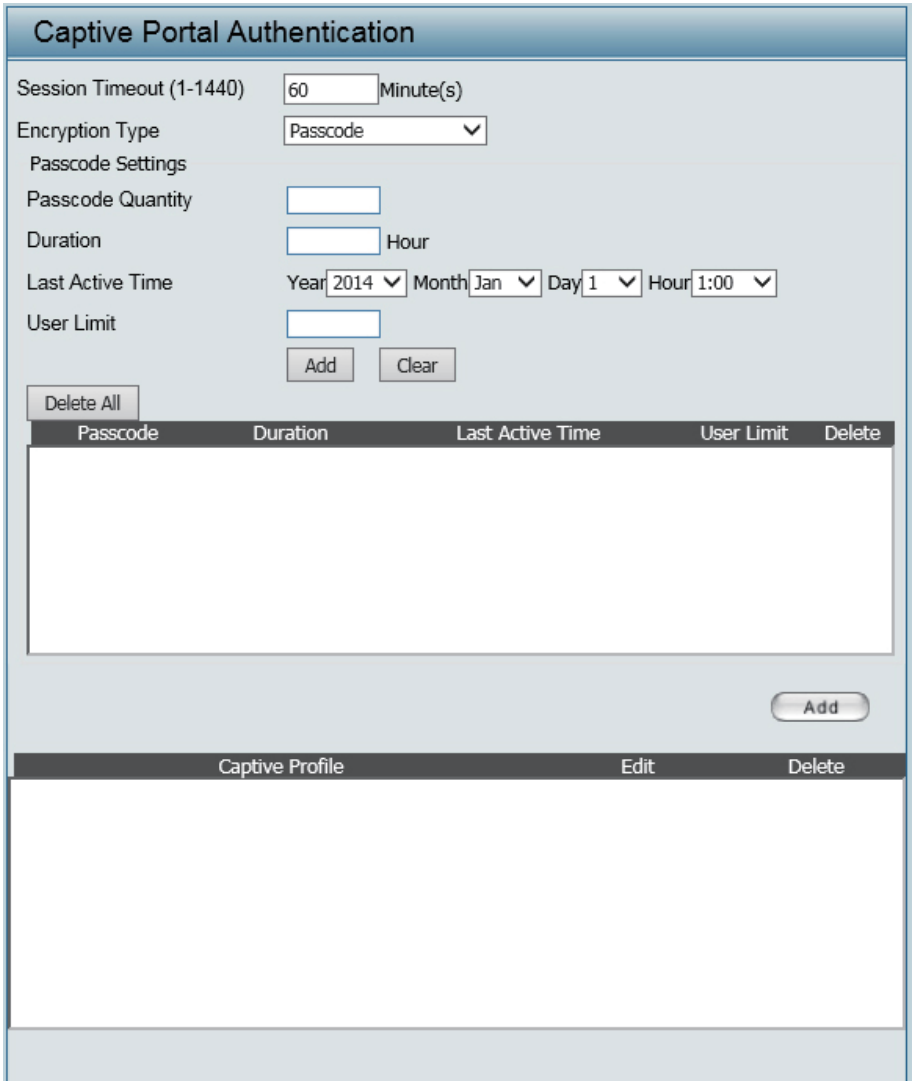
メモ

・Captive Portalを使う場合、クライアントは、APのManagement IPアドレスと同一セグメントである必要があります。

■Captive Portal Authentication（キャプティブポータル認証）

キャプティブポータル認証の暗号化タイプを選択し、各暗号化タイプごとに必要な設定を行います。

1. [Advanced Settings] > [Captive Portal] > [Authentication Settings] を選択します。
2. [Session Timeout] でセッションがタイムアウトする時間（分）を設定します。
3. [Encryption Type] で暗号化タイプを選択します。



4. 暗号化タイプごとに必要な設定を行います。

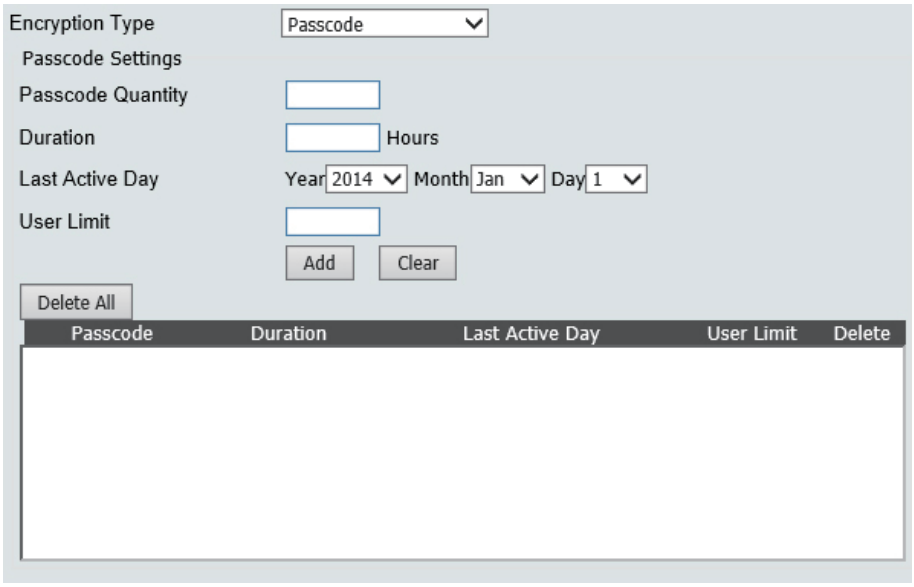
メモ

・選択した暗号化タイプによって設定項目が異なります。
・選択できる暗号化タイプは以下の通りです。
- Passcode → 『暗号化タイプを[Passcode]にした場合：p.56 』を参照
- Username/Password → 『暗号化タイプを[Username/Password]にした場合：p.57 』を参照
- Remote RADIUS → 『暗号化タイプを[Remote RADIUS]にした場合：p.58 』を参照
- LDAP → 『暗号化タイプを[LDAP]にした場合：p.58 』を参照
- POP3 → 『暗号化タイプを[POP3]にした場合：p.59 』を参照

● 暗号化タイプを[Passcode]にした場合

パスコードを使用して認証を行います。

1. 以下の画面でパスコードの設定を行います。



◆ **Passcode Quantitiy**	生成するパスコードの数を設定します。
◆ **Duration**	生成したパスコードを有効にする時間を設定します。
◆ **Last Active Day**	生成したパスコードが有効となる最終日（年/付/日）を設定します。
◆ **User Limit**	生成したパスコードを利用できるユーザ数の上限を設定します。
◆ **Add**	設定した内容を追加します。
◆ **Clear**	設定した内容を取り消します。
◆ **Delete All**	設定したパスコードすべてを削除します。

2. [Add]をクリックしてパスコード設定を追加します。

生成されたパスコードは以下のように表示されます。

Passcode	Duration	Last Active Day	User Limit	Delete
rjJfvoAf	1	2014-01-01	2	
4tUaJj7v	1	2014-01-01	2	
JOOrT2FN	1	2014-01-01	2	

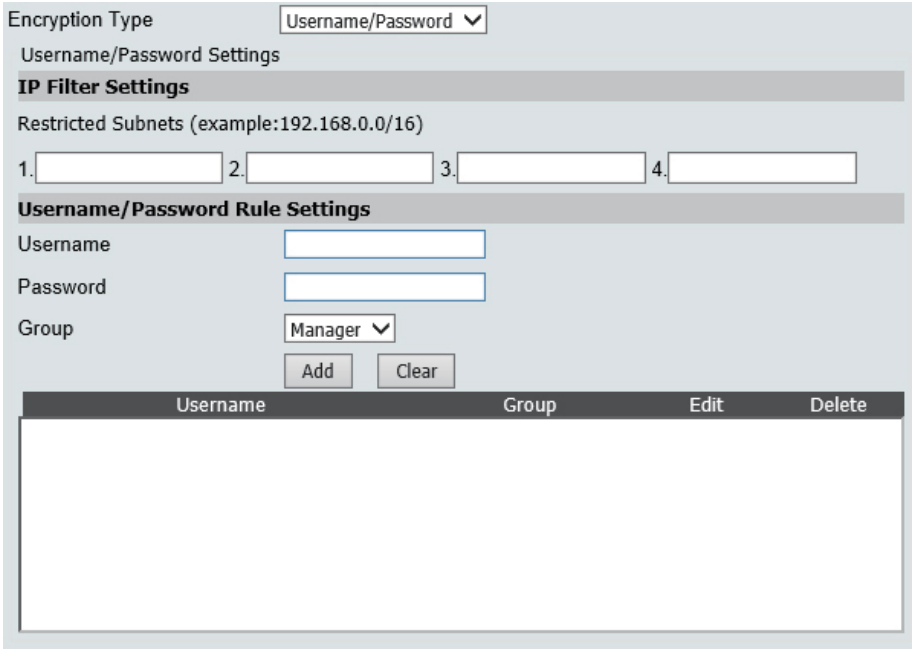
◎ パスコード設定を削除する場合：

1. [Delete]欄の🗑アイコンをクリックします。

● 暗号化タイプを[Username/Password]にした場合

ユーザ名とパスワードを使用して認証を行います。

1. 以下の画面でユーザ名とパスワードの設定を行います。



◆ **IP Filter Settings**	ゲストアカウントによる接続を禁止するサブネットを設定します。 • 記入例:192.168.0.0/16
◆ **Username/ Password Rule Settings**	アカウントの設定を行います。 • User Name : アカウントのユーザ名を入力します。 • Password : アカウントのパスワードを入力します。 • Group : アカウントのグループを[Manager](マネージャ)または[Guest](ゲスト)から選択します。[Guest](ゲスト)を選択した場合、[IP Filter Settings]で設定したサブネットにはアクセスできません。 • Add : 設定した内容を追加します。 • Clear : 設定した内容を取り消します。

2. [Add]をクリックしてユーザ名とパスワードの設定を追加します。

設定した内容は以下のように表示されます。

◎ ユーザ名とパスワードの設定を削除する場合:

1. [Delete]欄のアイコンをクリックします。

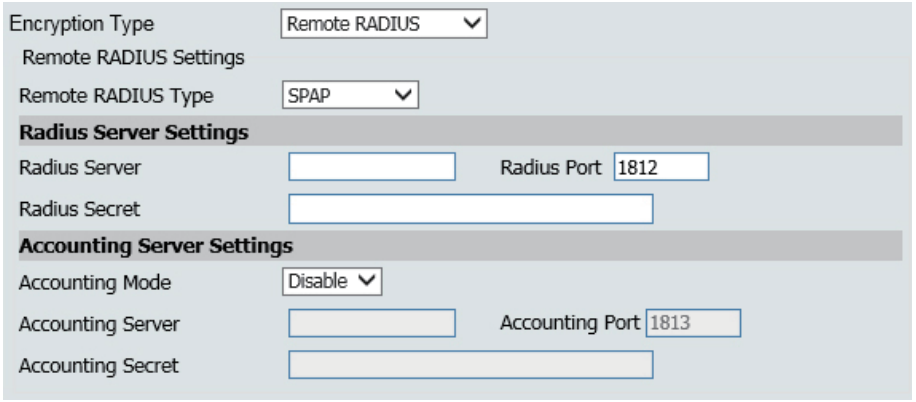
◎ ユーザ名とパスワードの設定を編集する場合:

1. [Edit]欄のアイコンをクリックします。
2. 設定を編集します
3. [Add]をクリックします。

● 暗号化タイプを[Remote RADIUS]にした場合

リモートRADIUSを使用して認証を行います。

1. 以下の画面でユーザ名とパスワードの設定を行います。

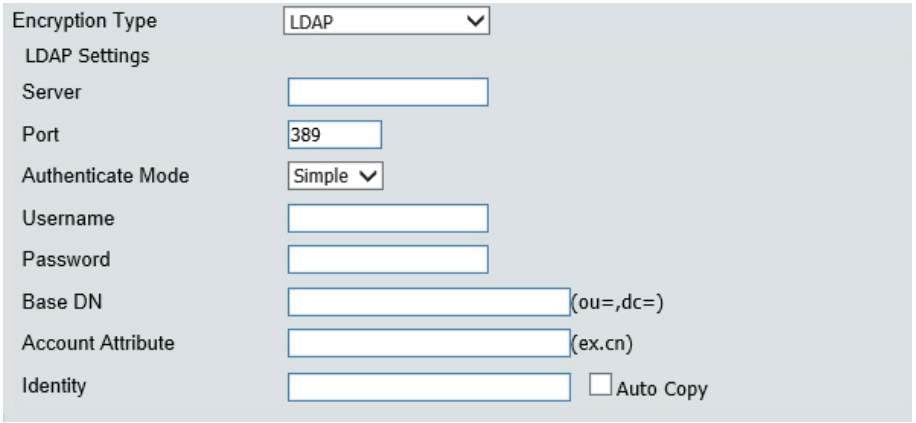


◆ **Remote RADIUS Type**	リモートRADIUSのタイプを以下から選択します。 • SPAP • MS-CHAPv2
◆ **Radius Server Settings**	RADIUSサーバの設定を行います。 • Radius Server : RADIUSサーバのIPアドレスを入力します。 • Radius Port : RADIUSサーバのポートを入力します。 初期値:1812 • Radius Secret: RADIUSシークレット(パスワード)を入力します。
◆ **Accounting Server Settings**	アカウンティングモードの設定を行います。 • Accounting Mode : アカウンテイングモードを[Enable](有効)または[Disable](無効)に設定します。 • Accouting Server : アカウンティングサーバのIPアドレスを入力します。 • Accounting Port : アカウンティングサーバのポートを入力します。 初期値:1813 • Accounting Secret : アカウンティングシークレット(パスワード)を入力します。

● 暗号化タイプを[LDAP]にした場合

LDAPサーバを使用して認証を行います。

1. 以下の画面でLDAPサーバの設定を行います。

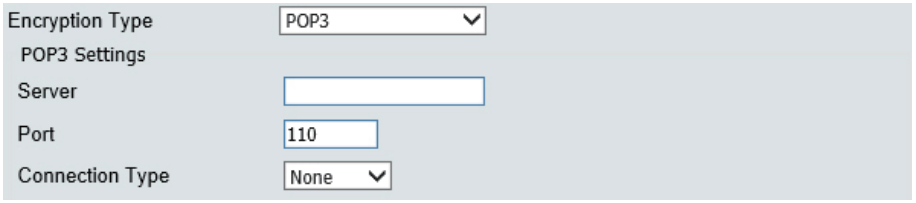


◆ **Server**	LDAPサーバのIPアドレスまたはドメイン名を入力します。
◆ **Port**	LDAPサーバのポートを入力します。 ・初期値：389
◆ **Authenticate Mode**	認証モードを選択します。 ・選択肢：[Simple][TLS]
◆ **Username**	LDAPサーバアカウントのユーザ名を入力します。
◆ **Password**	LDAPサーバアカウントのパスワードを入力します。
◆ **Base DN**	管理者のドメイン名を入力します。
◆ **Account Attribute**	LDAPアカウントに属するストリングを入力します。 このストリングはクライアントの検索に使用されます。
◆ **Identity**	アイデンティティのパスストリング全体を入力してください。 [Auto Copy]にチェックをいれると、自動的にパスが入力されます。

● 暗号化タイプを[POP3]にした場合

POP3サーバを使用して認証を行います。

1. 以下の画面でPOP3サーバの設定を行います。



◆ **Server**	POP3サーバのIPアドレスまたはドメイン名を入力します。
◆ **Port**	LDAPサーバのポートを入力します。 ・初期値：110
◆ **Connection Type**	接続モードを選択します。 ・選択肢：[None][SSL/TLS]

5. 画面下部の [Add] をクリックして、手順 3 で設定した内容をキャプティブプロファイルに追加ます。

設定した内容は以下のように表示されます。

◎ キャプティブプロファイル削除する場合：

1. [Delete]欄の アイコンをクリックします。

◎ キャプティブプロファイルを編集する場合：

1. [Edit]欄の アイコンをクリックします。
2. 設定を編集します。
3. [Add]をクリックして設定を保存します。

■Login Page Upload（ログイン画面アップロード）

キャプティブポータルのログイン画面に使用する画像をアップロードすることができます。

1. [Advanced Settings] > [Captive Portal] > [Login Page Upload] を選択します。
2. [参照] をクリックし、アップロードする画像を選択します。

メモ

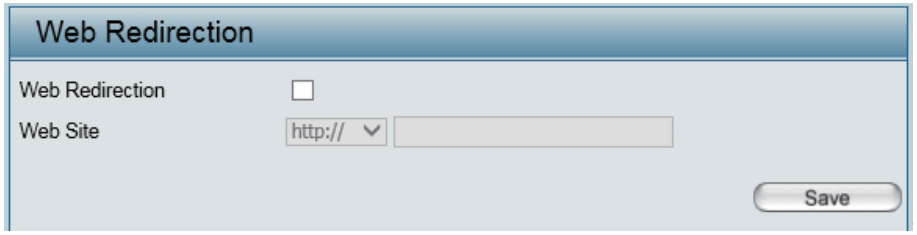
手動でパスを入力して画像を指定することもできます。

3. [Upload] をクリックして画像をアップロードします。

■Web Redirection（Webリダイレクション）

本項目では、Webリダイレクションの設定方法について説明します。
リダイレクトとは、サイトにアクセスしようとしたユーザーを、最初にリクエストされた URL とは別の URL に移動させることです。クライアントは、キャプティブポータルによる認証の際に本項目で設定したWebサイトにリダイレクトされます。

1. [Advanced Settings] > [Captive Portal] > [Web Redirect] を選択します。
2. [Web Redirection] にチェックをいれ、[Web Site] に Web サイトの URL を入力します。

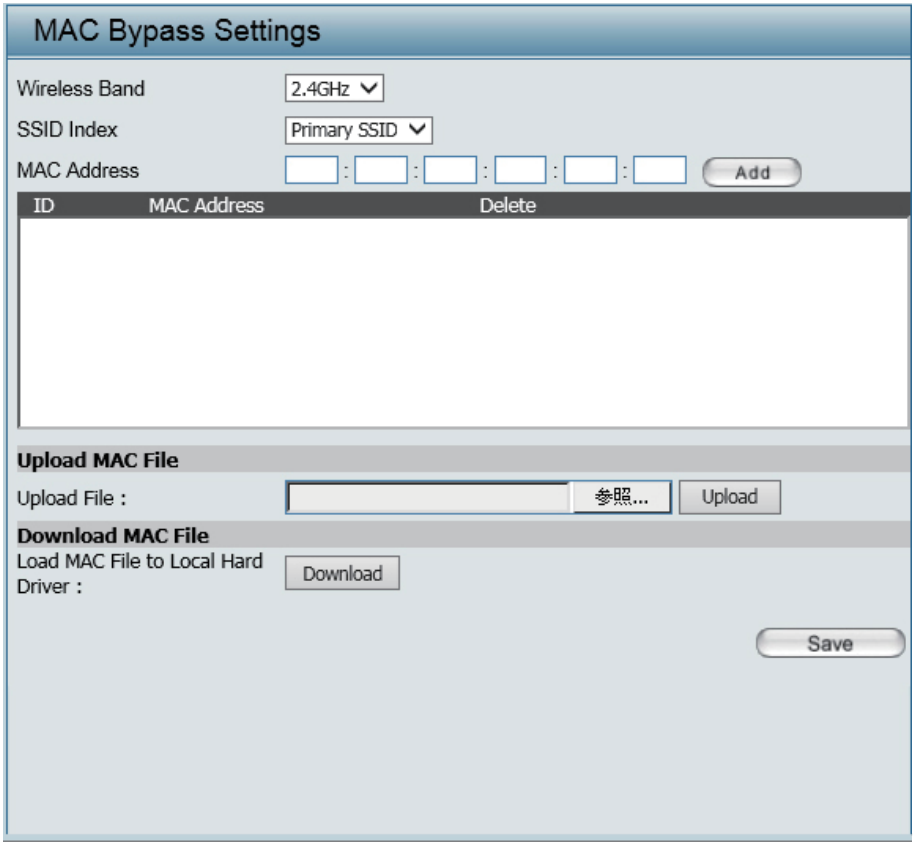


3. [Save] をクリックして設定を保存します。

■MAC Bypass Settings（MAC Bypass 設定）

本項目では、MAC Bypassの設定方法について説明します。

1. [Advanced Settings] > [Captive Portal] > [MAC Bypass Settings] を選択します。
2. 以下の画面で設定を行います。



◆ **Wireless Band**	周波数帯を[2.4GHz]または[5GHz]に設定します。
◆ **SSID Index**	SSIDを選択します。
◆ **MAC Address**	MACアドレスを入力し、[Add]をクリックします。 追加したMACアドレスは下の欄に表示されます。
◆ **Upload MAC File**	MACファイルのアップロードを行います。 [参照]をクリックしてMACファイルを選択→[Upload]をクリックします。
◆ **Download MAC File**	[Download]をクリックしMACファイルのダウンロードを行います。

3. [Save] をクリックして設定を保存します。

DHCP Server（DHCPサーバ設定）

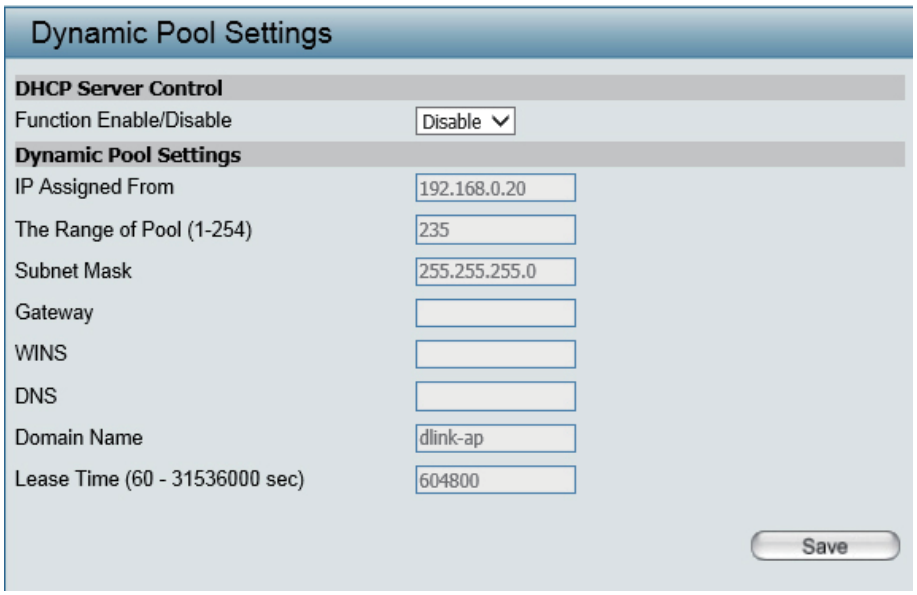
本製品のDHCP(Dynamic Host Configuration Protocol)サーバ機能の設定を行います。
DHCPサーバ機能により、IPアドレスなどネットワークに接続するために必要な情報を無線ステーションへ割り当てることができます。

■Dynamic Pool Settings（ダイナミックプール設定）

IPアドレスを自動的に無線ステーションへ割り当てるDHCPダイナミックプールの設定を行います。
DHCPアドレスプールは、ネットワークのステーションに割り当てるIPアドレスの範囲を定義します。
無線ステーションは、設定されたリース期間中、利用可能なIPアドレスを割り当てられます。

1. [Advanced Settings] > [DHCP Server] > [Dynamic Pool Settings] を選択します。

2. 以下の画面で設定を行います。



◆ **DHCP Server Control**	[Function Enable/Disable]でDHCPサーバ機能を有効または無効にします。 ・選択肢：[Enable]（有効）[Disable]（無効）
◆ **Dynamic Pool Settings**	DHCPサーバ機能を有効にした場合、以下の項目で設定を行います。 • IP Assigned From : 割り当てを開始するIPアドレスを入力します。 • The Range of Pool (1-254) : 割り当てが可能なIPアドレスの数を入力します。 選択可能範囲：1-254 • Subnet Mask : 割り当てるIPアドレスのサブネットマスクを入力します。 • Gateway : ゲートウェイIPアドレスを入力します。 • WINS : Windows Internet Naming Service (WINS)サーバのアドレスを入力します。 • DNS : Domain Name System (DNS)サーバのアドレスを入力します。 • Domain Name : ネットワークのドメイン名を入力します。 • Lease Time (60-31536000 sec): IPアドレスをリースする期間を入力します。リース期間を超過すると新しいIPアドレスが無線ステーションに割り当てられます。 選択可能範囲：60-31536000 (秒)

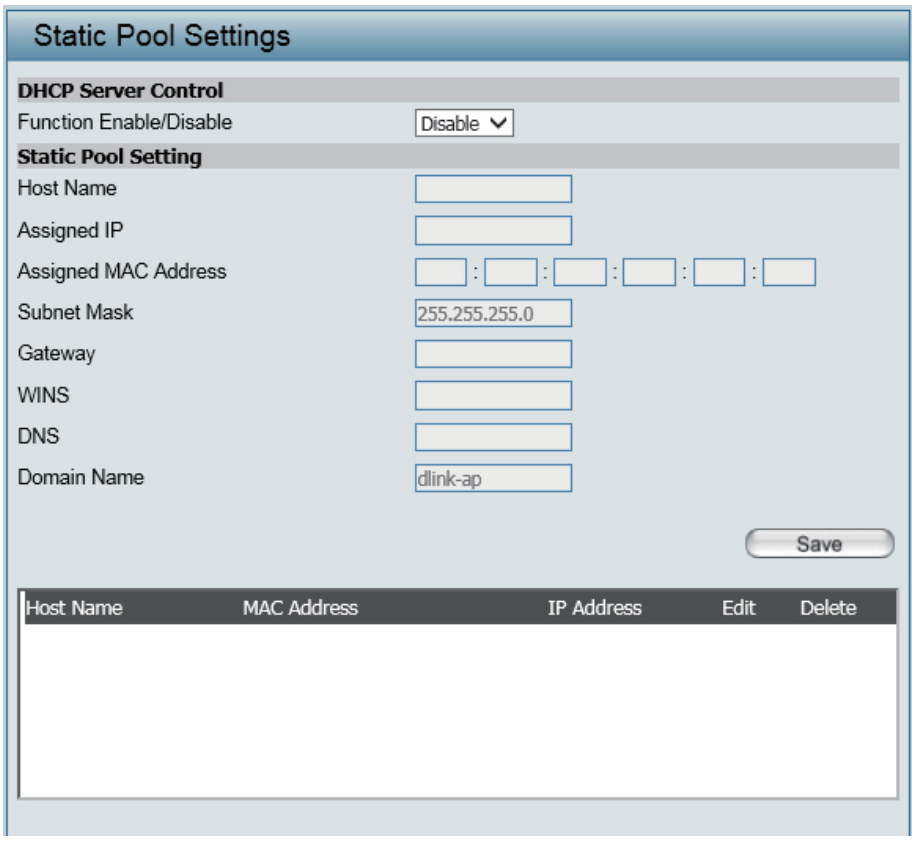
3. [Save] をクリックして設定を保存します。

■Static Pool Settings（スタティックプール設定）

固定のIPアドレスを無線ステーションへ割り当てるスタティックプールの設定を行います。

1. [Advanced Settings] > [DHCP Server] > [Static Pool Settings] を選択します。

2. 以下の画面で設定を行います。



◆ **DHCP Server Control**	[Function Enable/Disable]でDHCPサーバ機能を有効または無効にします。 • 選択肢：[Enable]（有効）[Disable]（無効）
◆ **Static Pool Settings**	DHCPサーバ機能を無効にした場合、以下の項目で設定を行います。 • Host Name : ホスト名を入力します。 • Assigned IP : 割り当てるIPアドレスを入力します。 • Assigned MAC Address : IPアドレスを割り当てる無線ステーションのMACアドレスを入力します。 • Subnet Mask : サブネットマスクを入力します。 • Gateway : ゲートウェイIPアドレスを入力します。 • WINS : Windows Internet Naming Service (WINS)サーバのアドレスを入力します。 • DNS : Domain Name System (DNS)サーバのアドレスを入力します。 • Domain Name : ネットワークのドメイン名を入力します。

◎ 設定を削除する場合：

1. [Delete]欄の アイコンをクリックします。

◎ 設定した内容を編集する場合：

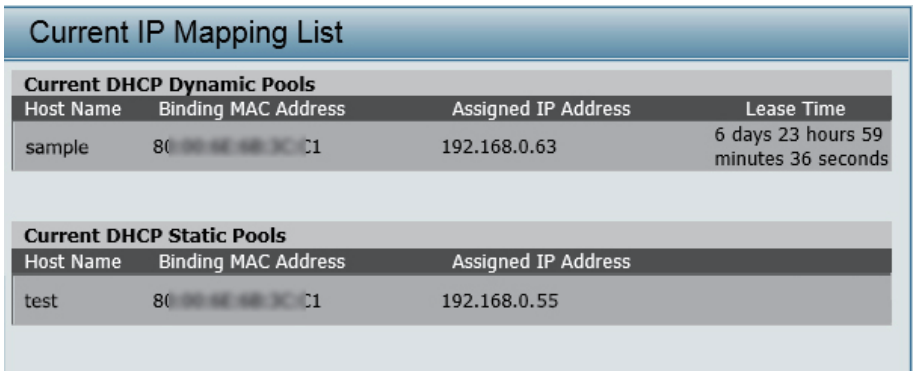
1. [Edit]欄の アイコンをクリックします。
2. 設定を編集します。
3. [Add]をクリックして設定を保存します。

3. [Save] をクリックして設定を保存します。

■Current IP Mapping List（IPマッピングリスト）

ダイナミックプール設定・スタティックプール設定によって割り当てられたIPアドレスのリストを表示します。

1. [Advanced Settings] > [DHCP Server] > [Static Pool Settings] を選択します。
2. 以下の画面で IP アドレスのリストを確認します。



◆ **Current DHCP Dynamic Pools**	ダイナミックプールで割り当てたIPアドレスのリストが表示されます。 • Host Name : ホスト名が表示されます。 • Binding MAC Address : IPアドレスを使用している無線ステーションのMACアドレスが表示されます。 • Assigned IP Address : 割り当てたIPアドレスが表示されます。 • Lease Time : IPアドレスのリース期間が表示されます。
◆ **Current DHCP Static Pools**	スタティックプールで割り当てたIPアドレスのリストが表示されます。 • Host Name : ホスト名が表示されます。 • Binding MAC Address : IPアドレスを使用している無線ステーションのMACアドレスが表示されます。 • Assigned IP Address : 割り当てたIPアドレスが表示されます。

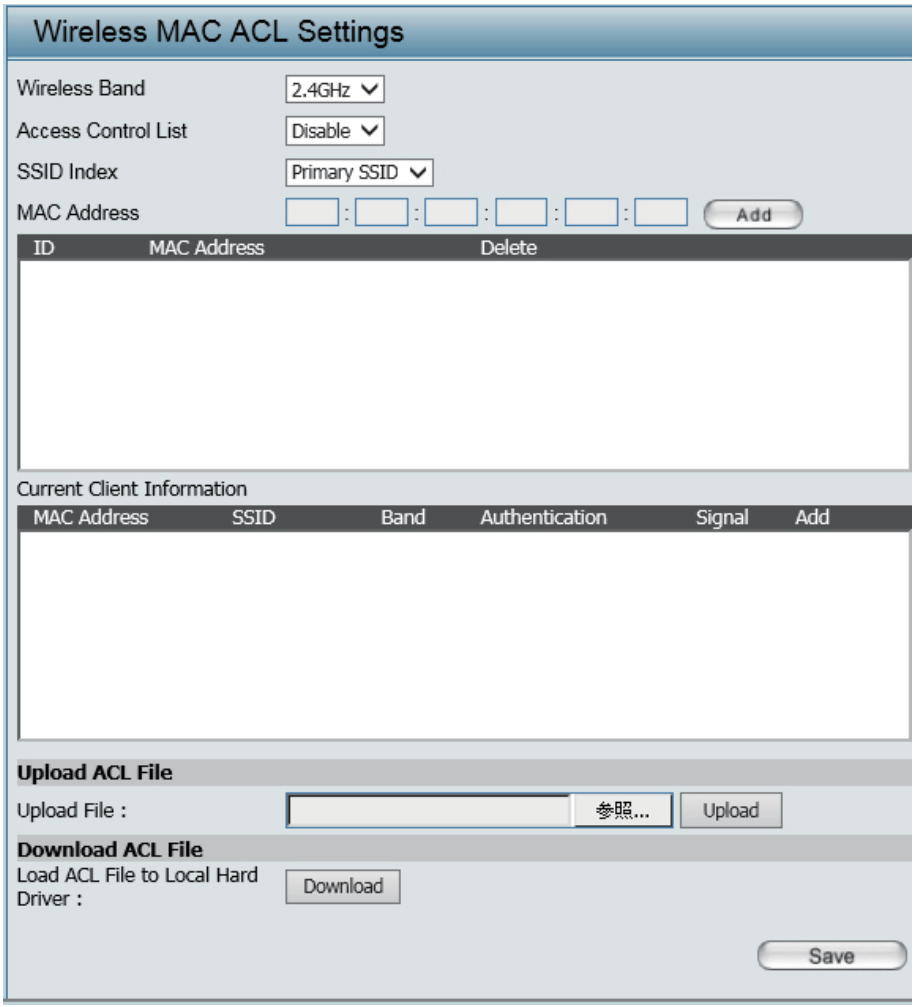
3. [Save] をクリックして設定を保存します。

Filters（フィルタ）

■Wireless MAC ACL Settings（ワイヤレスMAC ACL）

MACアドレスによるフィルタリングを行います。

1. [Advanced Settings] > [Filters] > [Wireless MAC ACL] を選択します。
2. 以下の画面で設定を行います。



◆ **Wireless Band**	周波数帯を[2.4GHz]または[5GHz]から選択します。
◆ **Access Control List**	ACL(Acceess Control List)の設定を無効/許可/拒否のいずれかに設定します。 • Disable : アクセスコントロールリストは無効となります。 • Accept : アクセスコントロールリストに登録されているMAC アドレスを持つデバイスのみ接続を許可します。 • Reject : アクセスコントロールリストに登録されているMAC アドレスを持つデバイスとの接続を拒否します。
◆ **SSID Index**	SSIDを選択します。
◆ **MAC Address**	以下の手順でMACアドレスを登録します。 1. MACアドレスを入力します。 2. [Add]をクリックします。
◆ **Current Client Information**	本製品に接続しているクライアントの情報が表示されます。 [Add]にチェックをいれると、クライアントはアクセスコントロールリストに追加されます。
◆ **Upload ACL File**	以下の手順でアクセスコントロールリストのファイルをアップロードします。 1. [参照]をクリックしてファイルを選択します。 2. [Upload]をクリックしてファイルをアップロードします。
◆ **Download ACL File**	[Download]をクリックして、アクセスコントロールリストのファイルをダウンロードします。

◎ アクセスコントロールリストを削除する場合：

1. [Delete]欄の🗑アイコンをクリックします。

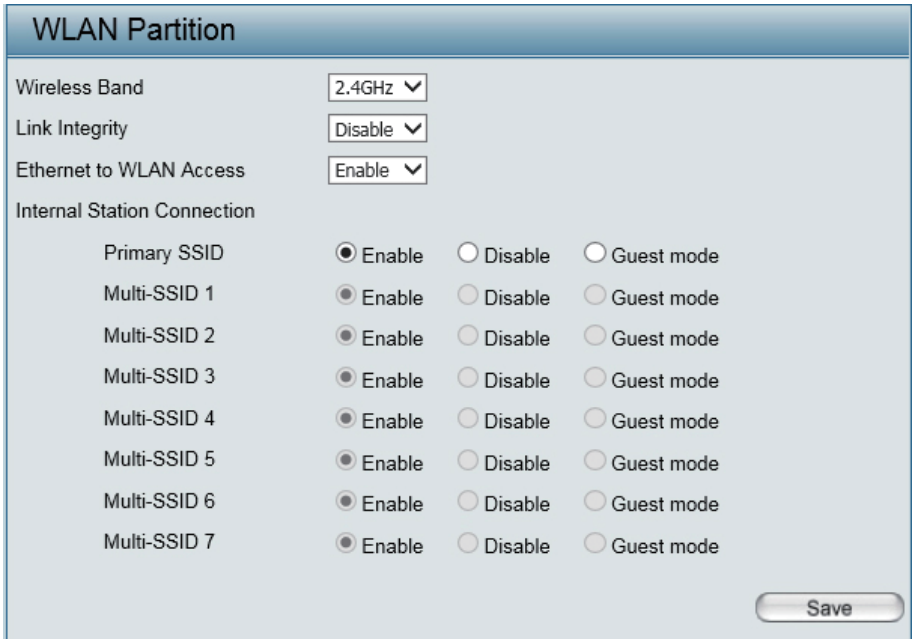
3. [Save] をクリックして設定を保存します。

■WLAN Partition（WLANパーティション）

WLANパーティションの設定を行います。

1. [Advanced Settings] > [Filters] > [WLAN Partition] を選択します。

2. 以下の画面で設定を行います。



◆ **Wireless Band**	周波数帯を[2.4GHz]または[5GHz]から選択します。
◆ **Link Integrity**	Link Integrity機能を有効または無効にします。 ・選択肢：[Enable]（有効）[Disable]（無効） Link Integrityは、複数の無線LANアクセスポイントを運用している場合に、発生したネットワーク障害を回避するための機能です。 LANとアクセスポイントが切断されると、ワイヤレスクライアントは自動的にそのアクセスポイントから切断されます。
◆ **Ethernet to WLAN Access**	有線LANから無線LANへのデータ送信を有効または無効にします。 ・選択肢：[Enable]（有効）[Disable]（無効） ・初期値：[Enable]
◆ **Internal Station Connection**	SSIDごとにステーションとの通信モードを設定します。 ・Enable： 同じSSIDに接続しているワイヤレスクライアント間での通信、および異なるSSIDに接続しているワイヤレスクライアント間での通信が可能です。 ・Disable： 同じSSIDに接続しているワイヤレスクライアント間での通信はできません。 異なるSSIDに接続しているワイヤレスクライアント間での通信は可能です。 ・Guest mode： 同じSSIDに接続しているワイヤレスクライアント間での通信、および異なるSSIDに接続しているワイヤレスクライアント間での通信ができません。

3. [Save] をクリックして設定を保存します。

Traffic Control（トラフィックコントロール）

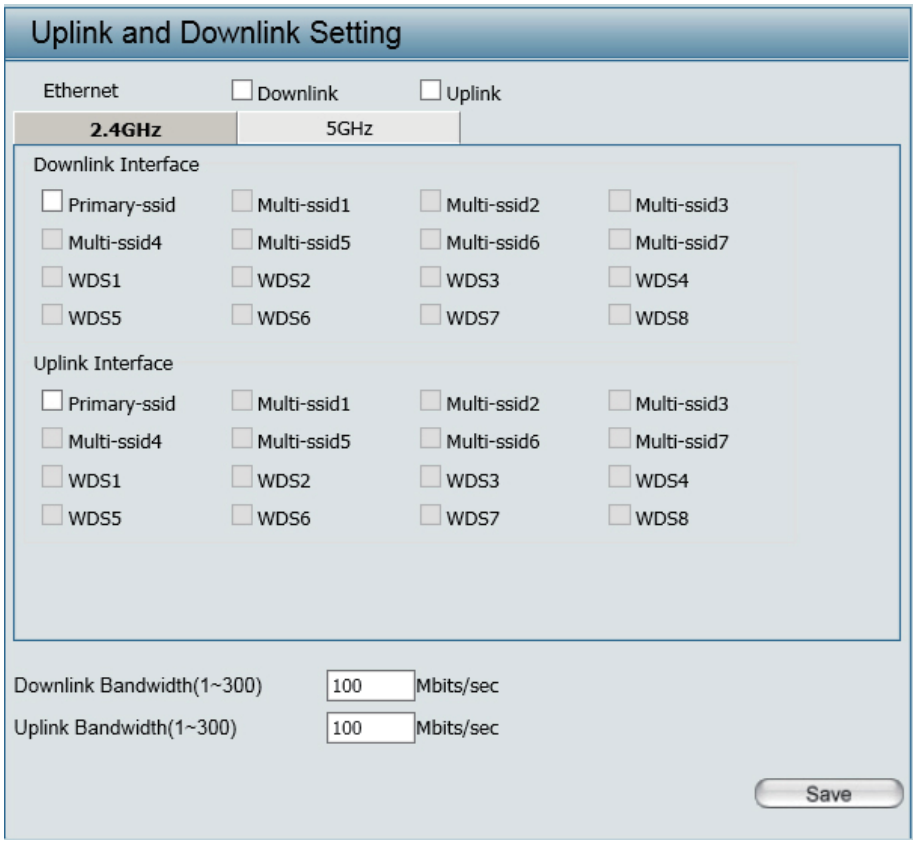
アップリンク/ダウンリンクの帯域幅設定、QoS設定などによりトラフィックをコントロールします。

■Uplink and Downlink Setting（アップリンク／ダウンリンク設定）

アップリンク/ダウンリンクの帯域幅を設定します。
本項目で設定した内容は、QoS及びTraffic Managerの設定内容にも反映されます。

1. [Advanced Settings] > [Traffic Control] > [Uplink/Downlink Settings] を選択します。

2. 以下の画面で設定を行います。



◆ **Ethernet**	[Downlink]または[Uplink]を選択します。
◆ **2.4GHz / 5GHz**	周波数帯を[2.4GHz]または[5GHz]から選択します。
◆ **Downlink Interface**	ダウンリンクインターフェースを選択します。
◆ **Uplink Interface**	アップリンクインターフェースを選択します。
◆ **Downlink Bandwidth (1-300)**	ダウンリンクの帯域幅を入力します。 ・選択可能範囲：1-300
◆ **Uplink Bandwidth (1-300)**	アップリンクの帯域幅を入力します。 ・選択可能範囲：1-300

3. [Save] をクリックして設定を保存します。

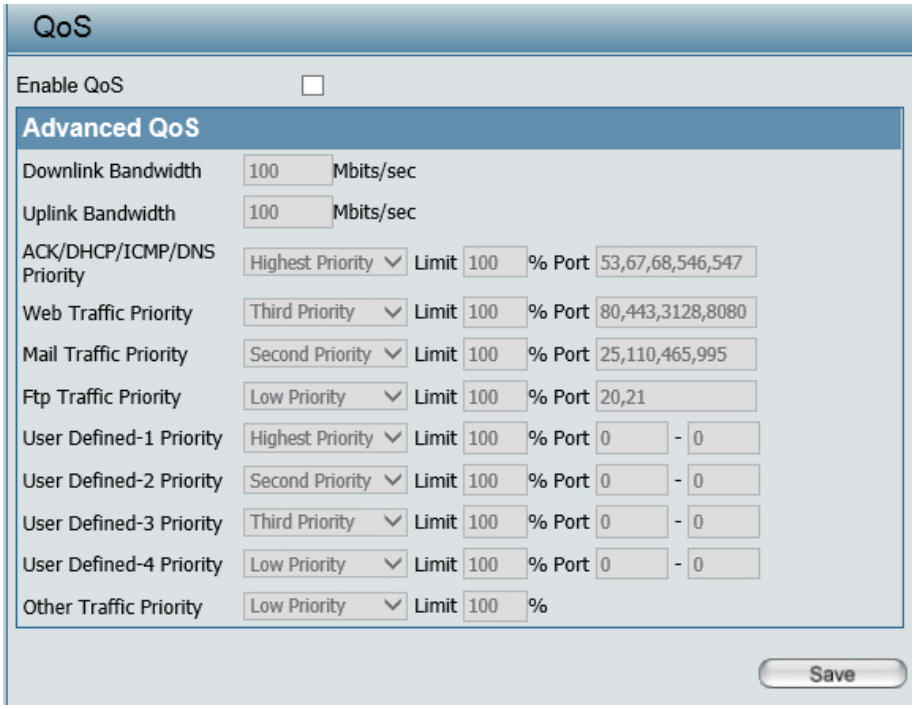
■QoS（QoS設定）

本項目ではQoSの設定を行います。

QoS (Quality of Servive) とは、各アプリケーションのトラフィックに優先順位を付けることで、ネットワークの利用を効率化する機能です。優先度を高く設定されたトラフィックが優先的に処理されます。

1. [Advanced Settings] > [Traffic Control] > [QoS] を選択します。

2. 以下の画面で設定を行います。


QoS
Enable QoS
Advanced QoS
Downlink Bandwidth 100 Mbits/sec
Uplink Bandwidth 100 Mbits/sec
ACK/DHCP/ICMP/DNS Priority Highest Priority Limit 100 % Port 53,67,68,546,547
Web Traffic Priority Third Priority Limit 100 % Port 80,443,3128,8080
Mail Traffic Priority Second Priority Limit 100 % Port 25,110,465,995
Ftp Traffic Priority Low Priority Limit 100 % Port 20,21
User Defined-1 Priority Highest Priority Limit 100 % Port 0 - 0
User Defined-2 Priority Second Priority Limit 100 % Port 0 - 0
User Defined-3 Priority Third Priority Limit 100 % Port 0 - 0
User Defined-4 Priority Low Priority Limit 100 % Port 0 - 0
Other Traffic Priority Low Priority Limit 100 %
Save

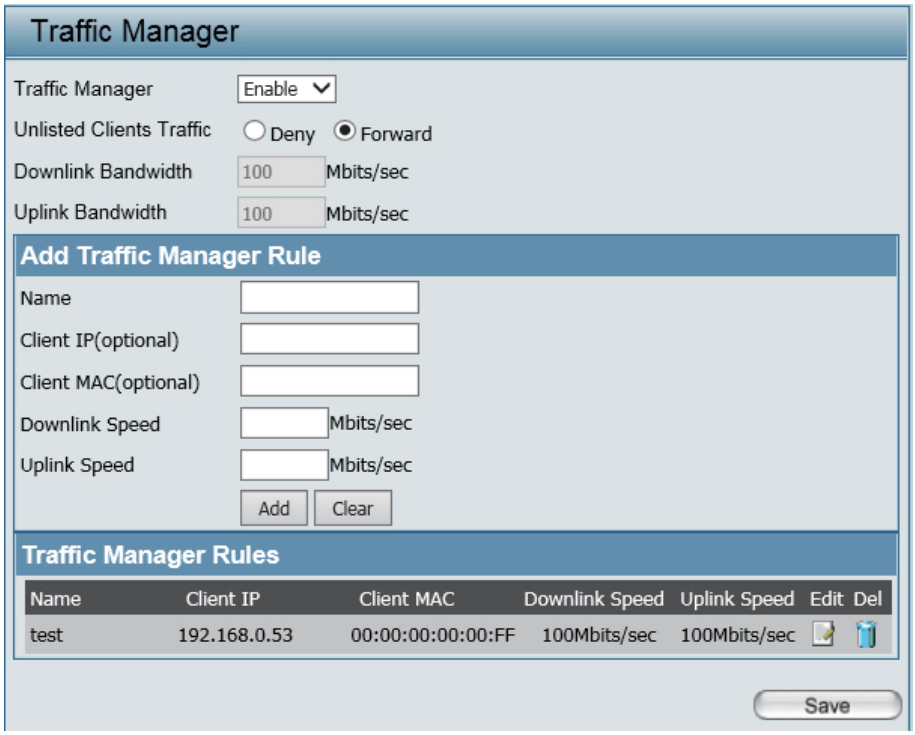
◆ **Enable QoS**	チェックをいれてQoSを有効にします。
◆ **Advanced QoS**	QoSの詳細設定を行います。 • Downlink Bandwidth : [Uplink and Downlink Setting]で設定した帯域幅が表示されます。 →『Uplink and Downlink Setting (アップリンク／ダウンリンク設定) : p.67 』 • Uplink Bandwidth : [Uplink and Downlink Setting]で設定した帯域幅が表示されます。 →『Uplink and Downlink Setting (アップリンク／ダウンリンク設定) : p.67 』 • Priority : 各トラフィックの優先度を設定します。 - Highest Priority : 最も高い優先度です。 - Second Priority : 2番目に高い優先度です。 - Third Priority : 3番目に高い優先度です。 - Low Priority : 最も低い優先度です。 • Limit : 各トラフィックのリミットを入力します。 • Port : 各トラフィックのポートを入力します。

3. [Save] をクリックして設定を保存します。

■Traffic Manager（トラフィックマネージャ）

トラフィックマネージャは、トラフィック管理ルールを作成し、クライアントのトラフィックとアップリンク／ダウンリンクのスピードを管理する機能です。

1. [Advanced Settings] > [Traffic Control] > [Traffic Manager] を選択します。
2. 以下の画面で設定を行います。



◆ **Traffic Manager**	トラフィックマネージャを有効または無効にします。 • 選択肢：[Enable]（有効）[Disable]（無効）
◆ **Unlisted Clients Traffic**	リストに登録されていないクライアントのトラフィックに対する対応を選択します。 • 選択肢：[Deny]（拒否）[Forward]（転送）
◆ **Downlink Bandwidth**	[Uplink and Downlink Setting]で設定した帯域幅が表示されます。 →『Uplink and Downlink Setting（アップリンク／ダウンリンク設定）：p.67 』
◆ **Uplink Bandwidth**	[Uplink and Downlink Setting]で設定した帯域幅が表示されます。 →『Uplink and Downlink Setting（アップリンク／ダウンリンク設定）：p.67 』
◆ **Add Traffic Manager Rule**	トラフィック管理ルールを作成します。 • Name：ルールの名前を入力します。 • Client IP (optional)：クライアントのIPアドレスを入力します。 • Client MAC (optional)：クライアントのMACアドレスを入力します • Downlink Speed：ダウンリンクの速度を入力します。（単位：Mbits/秒） • Uplink Speed：アップリンクの速度を入力します。（単位：Mbits/秒） • Add：設定した内容を追加します。 • Clear：設定した内容を取り消します。
◆ **Traffic Manager Rules**	作成したトラフィック管理ルールが表示されます。

◎ 設定を削除する場合：

1. [Del]欄の🗑アイコンをクリックします。

◎ 設定した内容を編集する場合：

1. [Edit]欄の📝アイコンをクリックします。
2. 設定を編集します。
3. [Add]をクリックして設定を保存します。

3. [Save] をクリックして設定を保存します。

Status（ステータス）

6

ファームウェアバージョンやクライアント情報、ログなど、アクセスポイントのステータスを確認できます。

■ Statusについて 71

■ Device Information（デバイス情報）..... 71

■ Client Information（クライアント情報）..... 72

■ WDS Information（WDS情報）..... 72

■ Channel Analyze（チャネル分析）..... 73

■ Statistics（統計情報）..... 74

Ethernet Traffic Statistics（イーサネットトラフィック統計情報）..... 74

WLAN Traffic Statistics（WLANトラフィック統計情報）..... 74

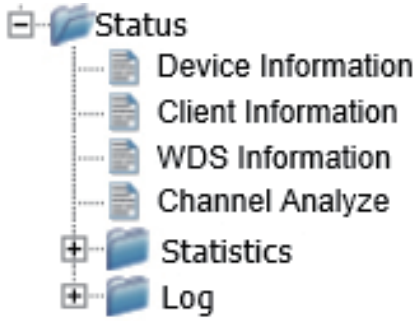
■ Log（ログ）..... 75

View Log（ログの表示）..... 75

Log Settings（ログ設定）..... 76

Statusについて

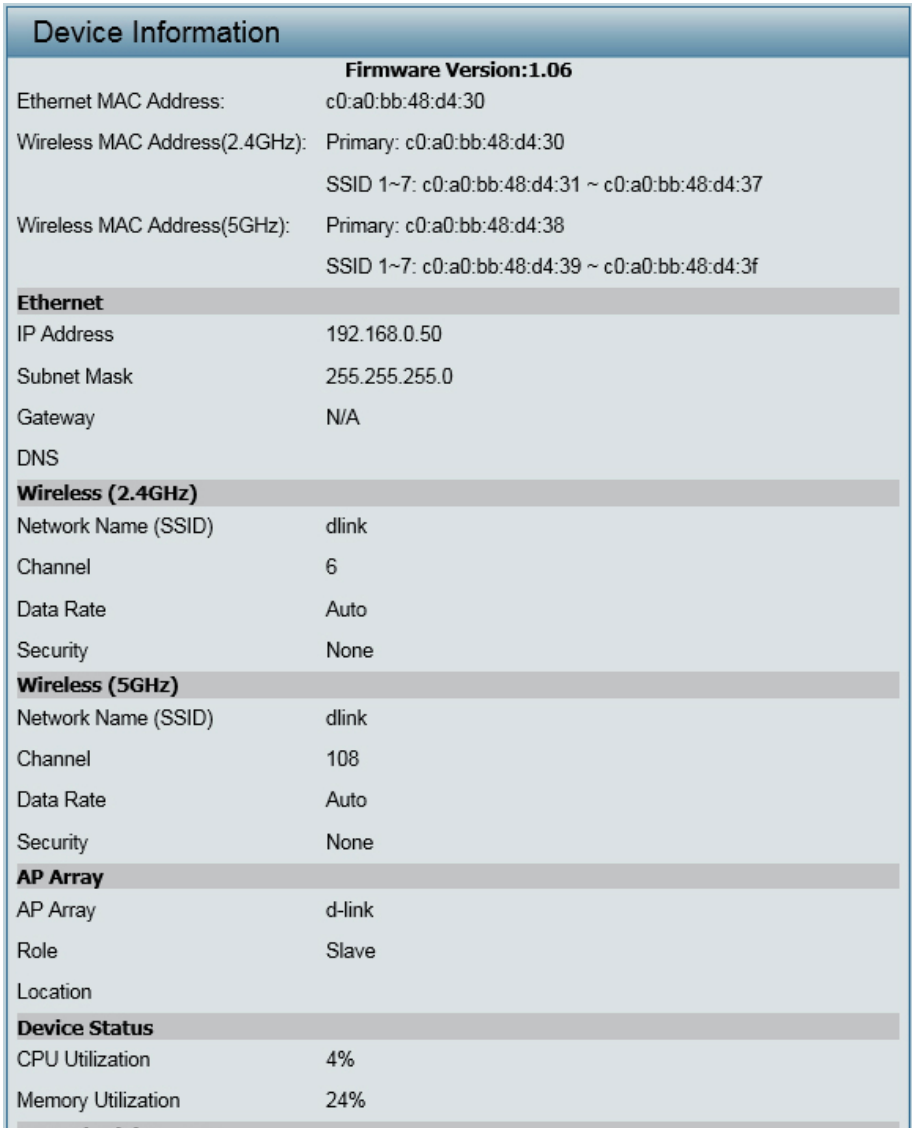
Status（ステータス）では、アクセスポイントのステータスを確認することができます。



Device Information（デバイス情報）

本製品の設定内容や、ファームウェアバージョン、MAC アドレスなどの情報が表示されます。

1. [Status] > [Device Information] を選択します。
2. 以下の画面で情報を確認します。



Device Information

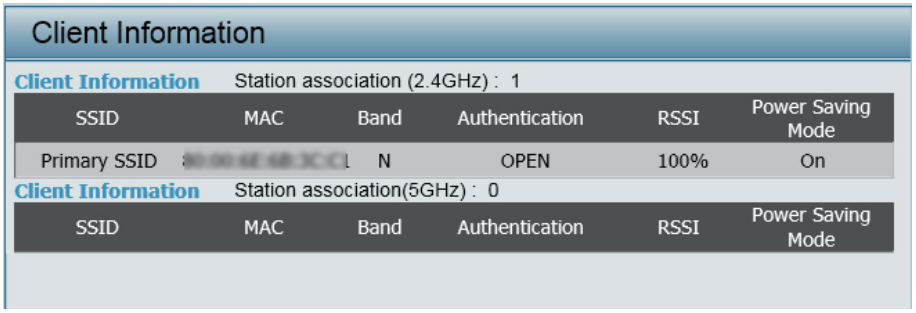
Firmware Version:1.06

Ethernet MAC Address:	c0:a0:bb:48:d4:30
Wireless MAC Address(2.4GHz):	Primary: c0:a0:bb:48:d4:30
	SSID 1~7: c0:a0:bb:48:d4:31 ~ c0:a0:bb:48:d4:37
Wireless MAC Address(5GHz):	Primary: c0:a0:bb:48:d4:38
	SSID 1~7: c0:a0:bb:48:d4:39 ~ c0:a0:bb:48:d4:3f
Ethernet	
IP Address	192.168.0.50
Subnet Mask	255.255.255.0
Gateway	N/A
DNS	
Wireless (2.4GHz)	
Network Name (SSID)	dlink
Channel	6
Data Rate	Auto
Security	None
Wireless (5GHz)	
Network Name (SSID)	dlink
Channel	108
Data Rate	Auto
Security	None
AP Array	
AP Array	d-link
Role	Slave
Location	
Device Status	
CPU Utilization	4%
Memory Utilization	24%

Client Information（クライアント情報）

本製品に接続しているクライアントの情報が、各帯域ごとに表示されます。

1. [Status] > [Client Information] を選択します。
2. 以下の画面で情報を確認します。

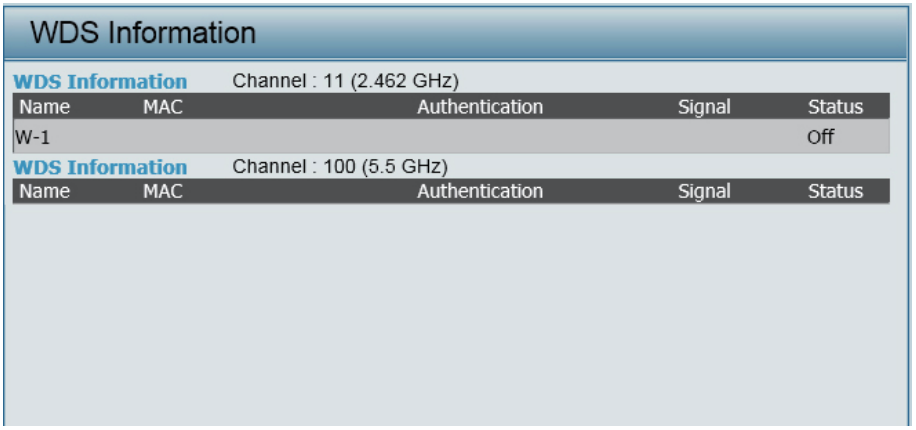


◆ **SSID**	クライアントのSSIDが表示されます。
◆ **MAC**	クライアントのMACアドレスが表示されます。
◆ **Band**	クライアントが接続している無線帯域が表示されます。
◆ **Authentication**	使用している認証方式が表示されます。
◆ **RSSI**	クライアントの受信信号強度（RSSI）が表示されます。
◆ **Power Saving Mode**	省電力モードの状態が表示されます。

WDS Information（WDS情報）

本製品に現在接続しているクライアントのWDS（アクセスポイント間接続）情報を表示します。

1. [Status] > [Client Information] を選択します。
2. 以下の画面で情報を確認します。

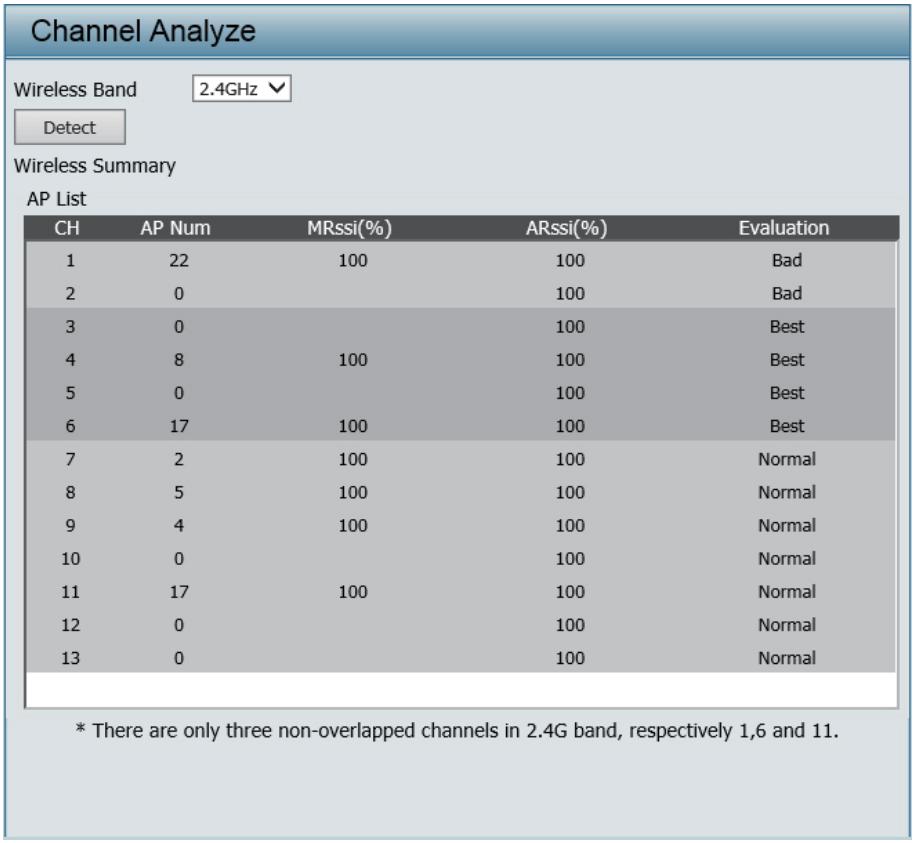


◆ **Name**	WDS名が表示されます。
◆ **MAC**	MACアドレスが表示されます。
◆ **Authentication**	使用している認証方式が表示されます。
◆ **Signal**	WDS リンクの信号強度が表示されます。
◆ **Status**	WDS接続の状態が表示されます。

Channel Analyze（チャネル分析）

アクセスポイントのチャンネル分析を行います。

1. [Status] > [Channel Analyze] を選択します。
2. [Detect] をクリックして検知を行い、以下の画面で情報を確認します。


Channel Analyze
Wireless Band
2.4GHz
Detect
Wireless Summary
AP List
CH AP Num MRssi(%) ARssi(%) Evaluation
1 22 100 100 Bad
2 0 100 Bad
3 0 100 Best
4 8 100 100 Best
5 0 100 Best
6 17 100 100 Best
7 2 100 100 Normal
8 5 100 100 Normal
9 4 100 100 Normal
10 0 100 Normal
11 17 100 100 Normal
12 0 100 Normal
13 0 100 Normal
* There are only three non-overlapped channels in 2.4G band, respectively 1,6 and 11.

◆ **Wireless Band**	周波数帯を[2.4GHz]または[5GHz]から選択します。
◆ **Detect**	チャンネルの検知を行います。
◆ **Wireless Summary**	チャネルの分析結果が表示されます。

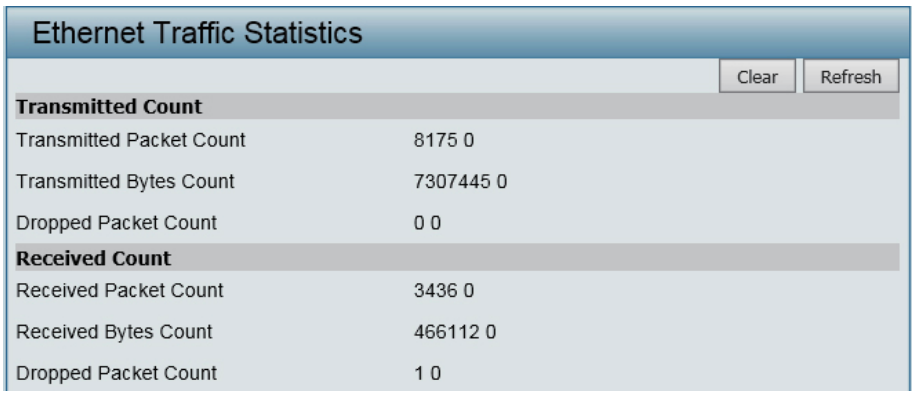
Statistics（統計情報）

■Ethernet Traffic Statistics （イーサネットトラフィック統計情報）

送受信されたパケットおよびバイトの統計情報を表示します。

1. [Status] > [Statistics] > [Ethernet] を選択します。

2. 以下の画面で情報を確認します。



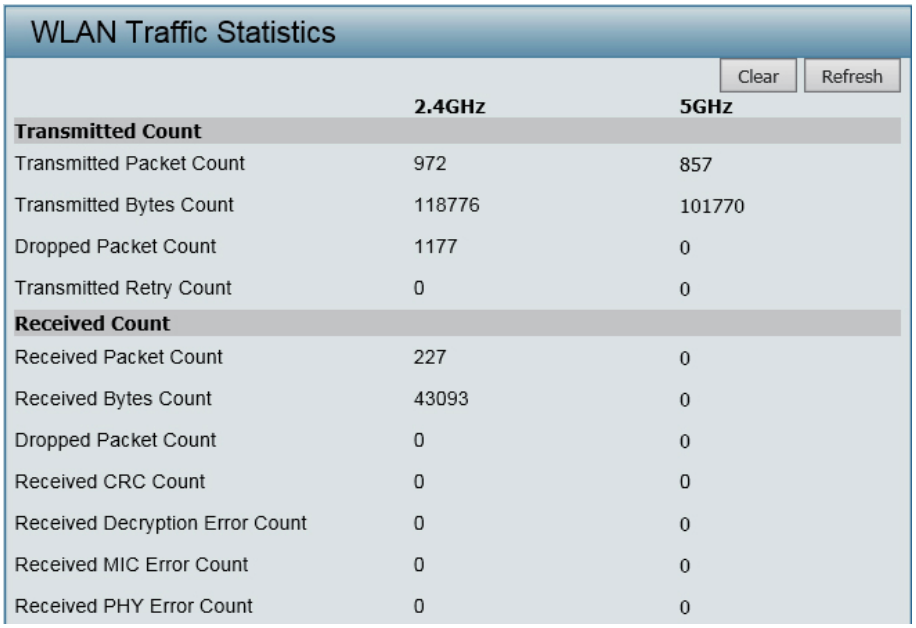
◆ **Clear**	統計情報を取り消します。
◆ **Refresh**	統計情報を更新します。
◆ **Transmitted Count**	送信した内容についての情報が表示されます。
◆ **Received Count**	受信した内容についての情報が表示されます。

■WLAN Traffic Statistics （WLANトラフィック統計情報）

無線ネットワークのデータスループット、送受信フレームおよびフレームエラーの統計情報を表示します。

1. [Status] > [Statistics] > [WLAN] を選択します。

2. 以下の画面で情報を確認します。



◆ **Clear**	統計情報を取り消します。
◆ **Refresh**	統計情報を更新します。
◆ **Transmitted Count**	送信した内容についての情報が表示されます。
◆ **Received Count**	受信した内容についての情報が表示されます。

Log（ログ）

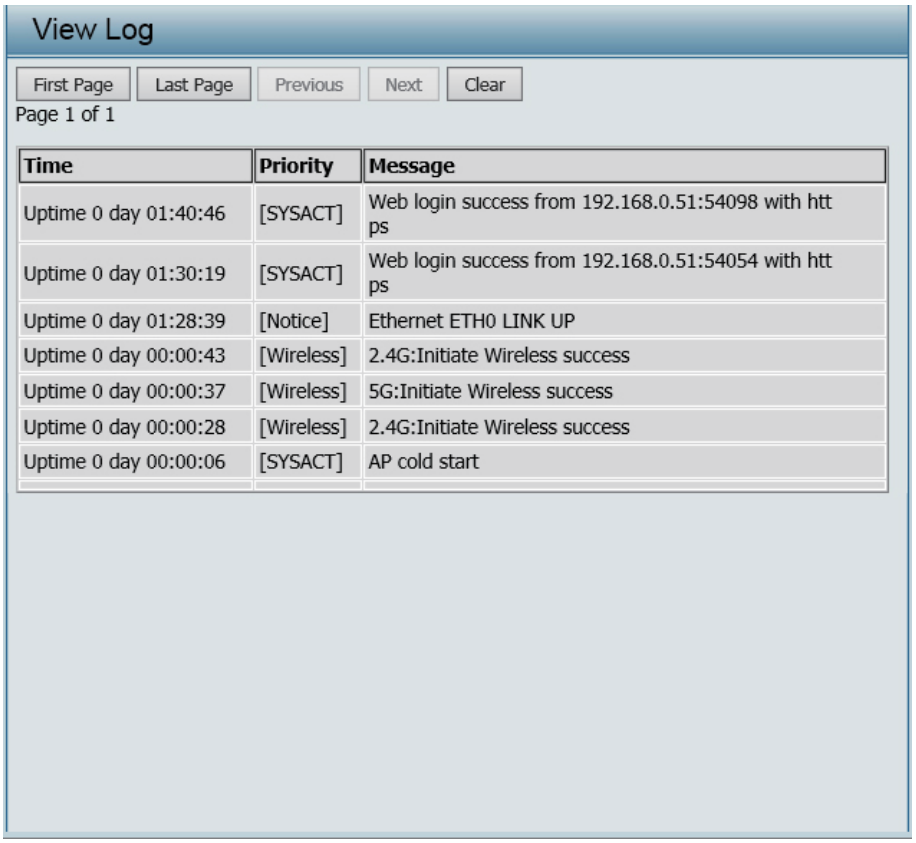
■View Log（ログの表示）

アクセスポイントの動作や無線LANクライアントとの接続記録などのログを表示します。

重要

保存できるログの数は500個までです。

1. [Status] > [Log] > [View Log] を選択します。
2. 以下の画面で情報を確認します。

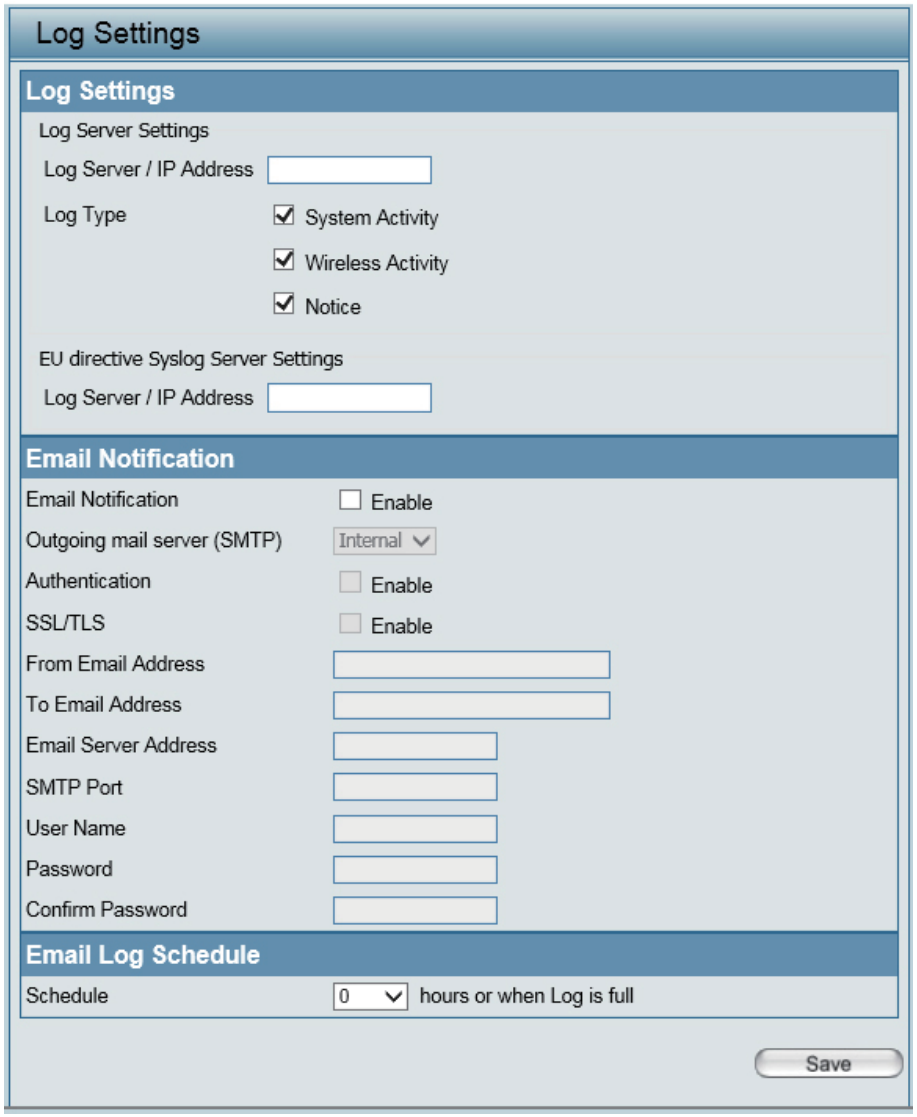


◆ **First Page** ◆ **Last Page**	最初のページ／最後のページを表示します。
◆ **Previous** ◆ **Next**	前のページ／次のページを表示します。
◆ **Clear**	ログを削除します。

■Log Settings （ログ設定）

ログ取得のための設定を行います。

1. [Status] > [Log] > [Log Settings] を選択します。
2. 以下の画面で設定を行います。



◆ **Log Settings**	ログを送信するサーバと送信するログのタイプを設定します。 • Log Server / IP Address : ログを送信するサーバのIP アドレスを入力します。 • Log Type: 送信するログのタイプを選択します。 - [System Activity] : ファームウェア更新などのログを取得します。 - [Wireless Activity] : 無線LAN クライアントの接続情報などのログを取得します。 - [Notice] : その他の情報のログを取得します。 • EU directive Syslog Server Settings: EU指令のSyslogサーバ設定を行います。
◆ **Email Notification**	ログのE-Mail通知を設定します。 • Email Notification : チェックをいれるとE-Mail通知が有効になります。 • Outgoing Mail Server (SMTP) : 送信用のSMTP サーバを以下から選択します。 - [Internal] [Gmail] [Hotmail] • Authentication : チェックをいれると認証が有効になります。 • SSL / TLS : チェックをいれるとSSL/TLS 認証が有効になります。 • From Email Address : E-mail/SMTP 送信元のE-mail アドレスを入力します。 • To Email Address : E-mail/SMTP 送信先のE-mail アドレスを入力します。 • Email Server Address : E-mail/SMTP サーバのIP アドレスを入力します。 • SMTP Port : SMTP ポートの番号を入力します。(初期値 : 25) • User Name : SMTP サーバのユーザ名を入力します。 • Password : SMTP サーバのパスワードを入力します。 • Confirm Password : 確認のためにSMTP サーバのパスワードを再度入力します。
◆ **Email Log Schedule**	ログのE-Mail通知を行う間隔を設定します (単位 : 時間)

3. [Save] をクリックして設定を保存します。

管理メニュー

7

ファームウェアアップデートや設定のリセットなど、本製品の管理を行う方法を説明します。

■ 管理メニューについて 79
Home 79
Maintenance 79
Configuration 79
System 79
Logout 79
Help 79
■ Home (ホーム画面) 79
■ Maintenance (メンテナンス) 80
Administration Settings (管理者設定) 80
Limit Administrator 81
System Name Settings 81
Login Settings 81
Console Settings 82
SNMP Settings 82
Ping Control Settings 82
LED Settings 82
Central WiFi Manager 82
Firmware Upload (ファームウェアとSSL証明書のアップロード) 83
ファーウェアのアップロード 83
SSL証明書のアップロード 83
Configuration File Upload and Download
(コンフィグレーションファイルのアップロードとダウンロード) 84
コンフィグレーションのアップロード 84
コンフィグレーションのダウンロード 84
Time and Date Settings (時刻と日付の設定) 85
■ Configuration (コンフィグレーション) 86
設定の保存と有効化 86
設定の破棄 86
■ System (システム設定) 87
本製品の再起動 87
工場出荷時設定へのリセット 87
■ Logout (ログアウト) 88
■ Help (ヘルプ) 88

管理メニューについて

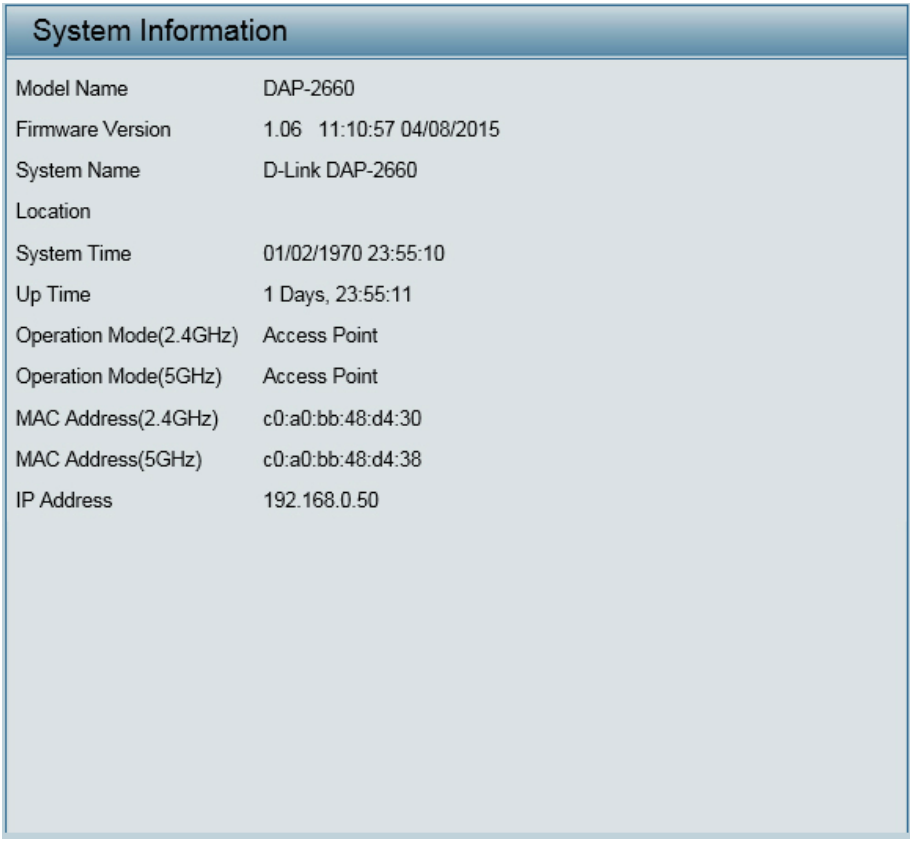
ファームウェアアップデートや設定の保存、リセットなどを行うことができます。
管理メニューには以下の項目があります。

- Home
  System Information(システム情報)画面を表示します。
  『Home (ホーム画面) : p.79 』
- Maintenance
  管理者設定やファームウェアアップグレードなど、本製品のメンテナンスを行います。
  『Maintenance (メンテナンス) : p.80 』
- Configuration
  設定の保存・有効化と、設定変更の取り消しを行います。
  『Configuration (コンフィグレーション) : p.86 』
- System
  本製品の再起動と、工場場出荷時状態へのリセットを行います。
  『System (システム設定) : p.87 』
- Logout
  WebGUI画面からログアウトします。
  『Logout (ログアウト) : p.88 』
- Help
  ヘルプ画面を表示します。
  『Help (ヘルプ) : p.88 』

Home (ホーム画面)

System Information (システム情報)画面を表示します。

1. [Home] アイコンをクリックします。
2. 以下の画面で情報を確認します。



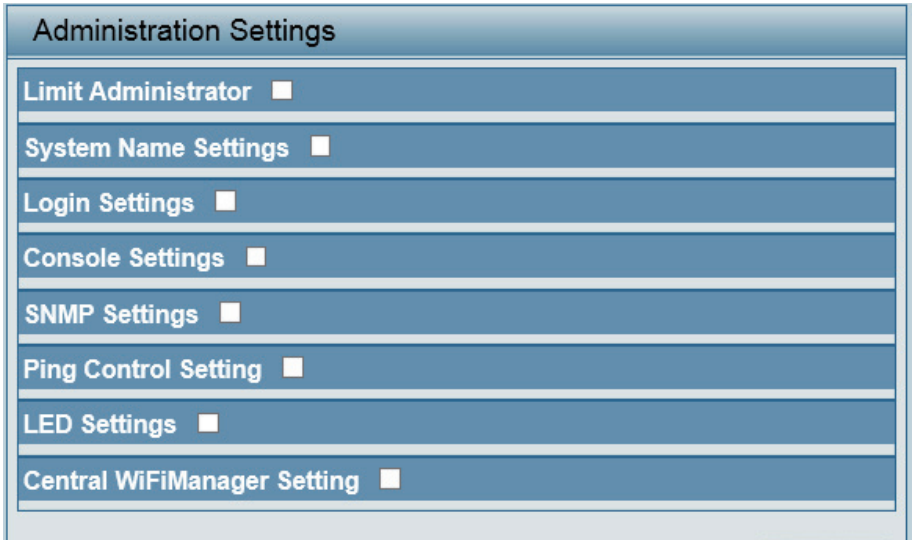
Maintenance（メンテナンス）

■Administration Settings （管理者設定）

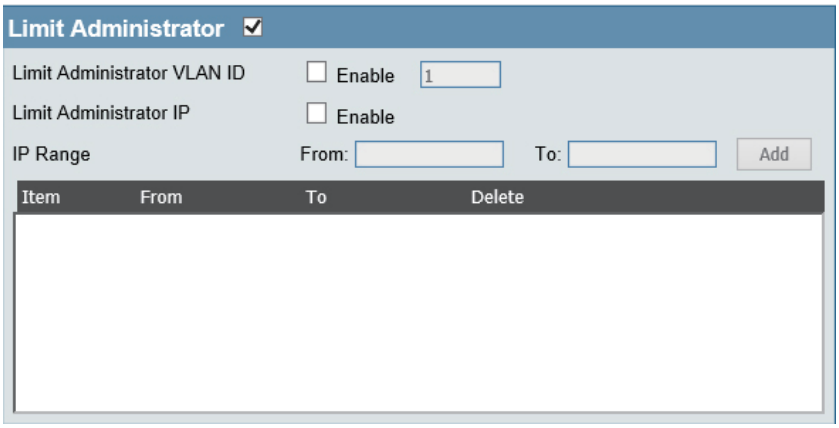
ログイン設定やコンソール設定など、管理者設定を行います。
管理者設定には以下の項目があります。

- Limit Administrator (管理者の制限)
  →『Limit Administrator：p.81 』を参照
- System Name Settings（システム名設定）
  →『System Name Settings：p.81 』を参照
- Login Settings（ログイン設定）
  →『Login Settings：p.81 』を参照
- Console Settings（コンソール設定）
  →『Console Settings：p.82 』を参照
- SNMP Settings（SNMP設定）
  →『SNMP Settings：p.82 』を参照
- Ping Control Setting（Ping管理設定）
  →『Ping Control Settings：p.82 』を参照
- Central WiFiManager Setting（WiFIマネージャ設定）
  →『Central WiFi Manager：p.82 』を参照

1. [Maintenance] アイコンをクリック→ [Administration Settings] を選択します。
2. 以下の画面で項目を選択し、設定を行います。



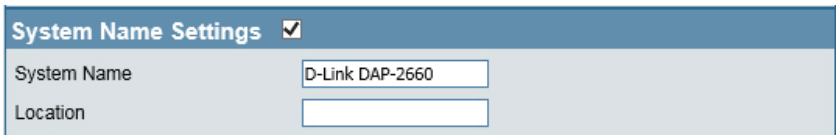
● Limit Administrator
管理者の制限を行います。



◆ **Limit Administrator VLAN ID**	[Enable] をチェックし、管理者がログインできるVLAN ID を入力します。
◆ **Limit Administrator IP**	[Enable] をチェックし、管理者がログインできるIPアドレスを制限します。
◆ **IP Range**	[Limit Administrator IP]を有効にした場合、管理者がログインできるIPアドレス範囲を入力します。
◆ **Add**	設定したIPアドレス範囲を追加します。

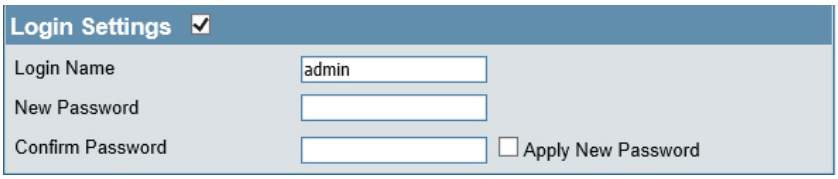
◎ IPアドレス範囲を削除する場合：
1. [Delete]欄のアイコンをクリックします。

● System Name Settings
システム名を設定します。



◆ **System Name**	本製品のシステム名を入力します。 ・初期値：D-Link DAP-2660
◆ **Location**	本製品の設置場所を入力します。

● Login Settings
Web GUIにログインする場合の情報をログイン名とパスワードを設定します。

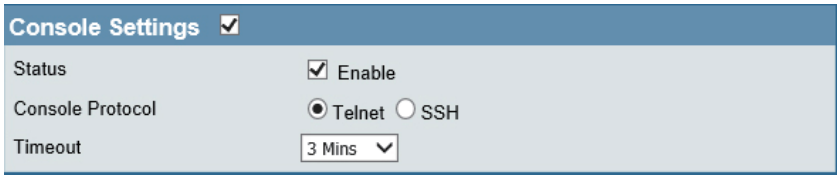


◆ **Login Name**	ログイン名を入力します。 ・初期値：admin
◆ **New Password**	新しいパスワードを入力します。　入力可能文字数：12文字以内 ・初期値：空欄
◆ **Confirm Password**	確認のため、新しいパスワードを再度入力します。
◆ **Apply New Password**	チェックをいれると新しいパスワードが有効になります。

重要

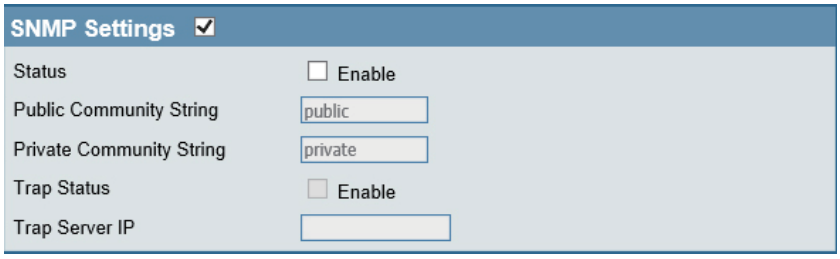
パスワードは大文字と小文字が区別されます。

● Console Settings
Web GUIにログインする場合の情報をログイン名とパスワードを設定します。



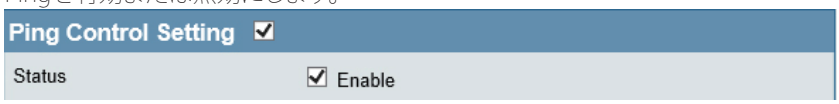
◆ **Status**	[Enable] をチェックし、コンソール接続を有効にします。
◆ **Console Protocol**	コンソール接続で使用するプロトコルを選択します。 ・初期値：Telnet
◆ **Timeout**	タイムアウトの設定を選択します。 ・選択肢：[1 Min][3 Mins][5 Mins][10 Mins][15 Mins][Never]

● SNMP Settings
SNMPの設定を行います。



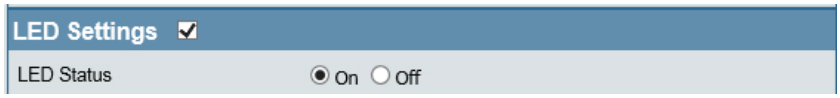
◆ **Status**	[Enable] をチェックし、SNMPを有効にします。
◆ **Public Community String**	パブリックSNMP コミュニティ名を入力します。 ・初期値：public
◆ **Private Community String**	プライベートSNMP コミュニティ名を入力します。 ・初期値：private
◆ **Trap Status**	[Enable] をチェックし、トラップを有効にします。
◆ **Trap Server IP**	トラップサーバのIP アドレスを入力します。

● Ping Control Settings
Pingを有効または無効にします。



◆ **Status**	[Enable] をチェックし、Pingを有効にします。

● LED Settings
LEDをオンまたはオフにします。



◆ **LED Status**	[On]または[Off]を選択します。

● Central WiFi Manager
WiFiマネージャの設定を行います。

◆ **Enable Central WiFi Manager**	WiFiマネージャを有効または無効に設定します。 ・選択肢：[Enable]（有効）[Disable]（無効）

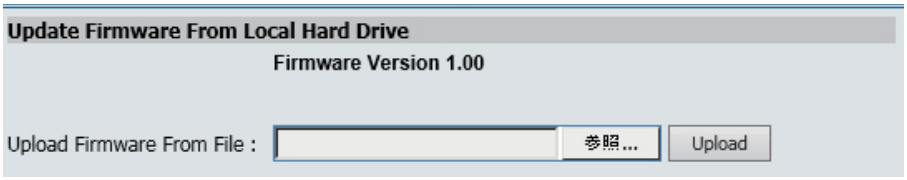
3. [Save] をクリックして設定を保存します。

■Firmware Upload（ファームウェアとSSL証明書のアップロード）

ファームウェアおよびSSL証明書のアップロードを行います。

● ファーウェアのアップロード

1. [Maintenance] アイコンをクリック→ [Firmware Upload] を選択します。
2. 以下の画面で [参照] をクリックしてローカルに保存したファームウェアを指定します。



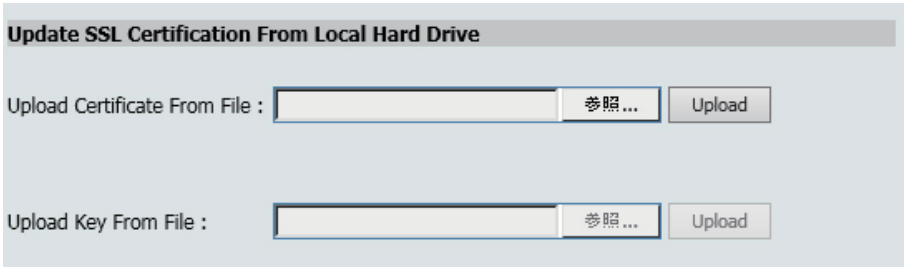
3. [Upload] をクリックします。

⚠注意

アップロード中に電源を切らないでください。
アップデート中に電源を切ると、起動に失敗し、正常に起動できなくなることがあります。故障の原因となりますので、ご注意ください。

● SSL証明書のアップロード

1. [Maintenance] アイコンをクリック→ [Firmware Upload] を選択します。
2. 以下の画面で [参照] をクリックし、ファイルを選択 します。



◆ **Upload Certificate From File**	更新する証明書を指定します。
◆ **Upload Key From File**	更新する認証キーを指定します。

3. [Upload] をクリックします。

■Configuration File Upload and Download （コンフィグレーションファイルのアップロードとダウンロード）

コンフィグレーションファイルのアップロードとダウンロードを行います。

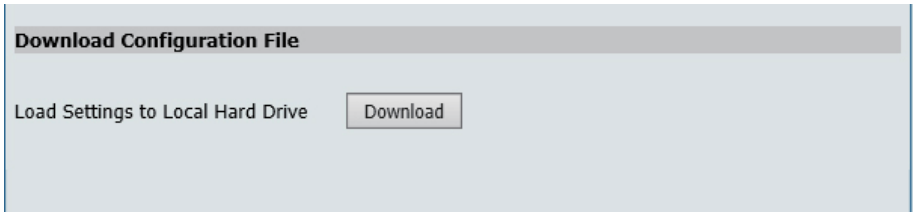
● コンフィグレーションのアップロード

1. [Maintenance] アイコンをクリック→ [Configuration File] を選択します。
2. 以下の画面で [参照] をクリックしてをファイルを選択 します。

3. [Upload] をクリックします。

● コンフィグレーションのダウンロード

1. [Maintenance] アイコンをクリック→ [Configuration File] を選択します。
2. 以下の画面で [Download] をクリックし、ファイルをダウンロードします。

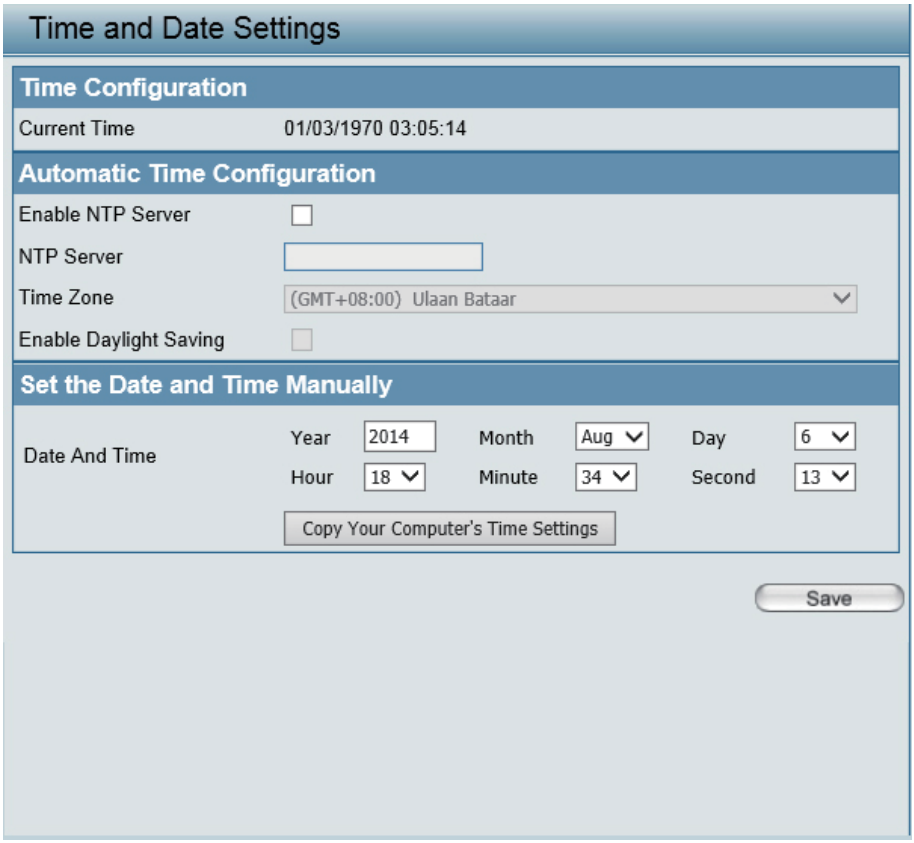


■Time and Date Settings（時刻と日付の設定）

本製品の時刻の設定を行います。
NTPサーバを使用して自動的に日時を設定、または手動で日時を設定することができます。

1. [Maintenance] アイコンをクリック→ [Time and Date] を選択します。

2. 以下の画面で設定を行います。



◆ **Time Configuration**	[Current Time]に現在設定されている日時が表示されます。
◆ **Automatic Time Configuration**	NTPサーバを使用して自動的に日時を設定します • Enable NTP Server : チェックをいれるとNTPサーバが有効になります。 • NTP Server : NTPサーバのIPアドレスを入力します。 • Time Zone : タイムゾーンを設定します。 • Daylight Saving Time : チェックをいれるとサマータイムが有効になります
◆ **Set the Date and Time Manually**	日付と時刻設定します。 • Date and Time : 日付と時刻を入力します。 • Copy Your Computer's Time Settings : クリックすると、お使いのPCの日時をコピーできます。

3. [Save] をクリックして設定を保存します。

Configuration（コンフィグレーション）

■設定の保存と有効化

設定した内容を保存・有効化します。

1. [Configuration] アイコンをクリック→ [Save and Active] を選択します。
2. 以下の画面が表示され、設定の保存と有効化が行われます。

⚠注意

再起動中は、電源を切らずにそのままお待ちください。

■設定の破棄

設定した内容を破棄します。

1. [Configuration] アイコンをクリック→ [Discard Changes] を選択します。
2. 以下の画面が表示され、設定の破棄が行われます。

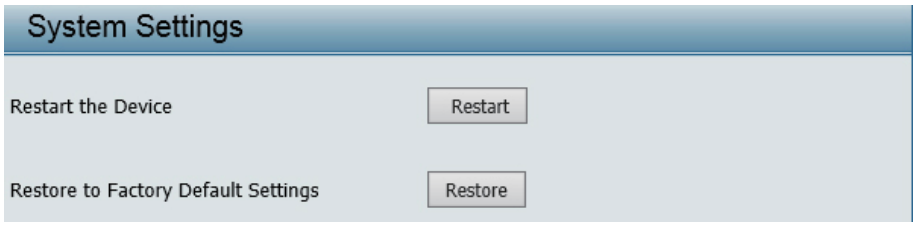
⚠注意

再起動中は、電源を切らずにそのままお待ちください。

System （システム設定）

■本製品の再起動

1. [System] アイコンをクリックします。
2. [Restart] をクリックします。



3. 確認画面が表示されるので、[OK] をクリックします。
4. 以下の画面が表示され、再起動が行われます。

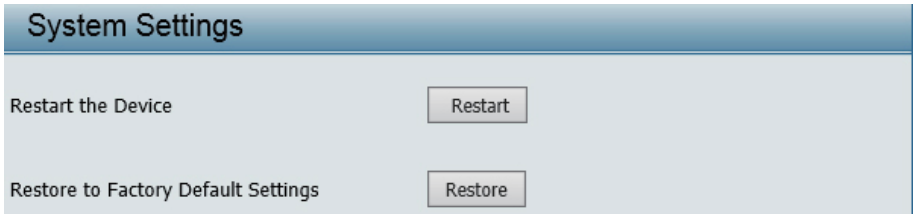
⚠注意

再起動中は、電源を切らずにそのままお待ちください。

■工場出荷時設定へのリセット

工場出荷時の状態へ設定をリセットします。

1. [System] アイコンをクリックします。
2. [Restore] をクリックします。



3. 以下の画面が表示され、再起動が行われます。

⚠注意

再起動中は、電源を切らずにそのままお待ちください。

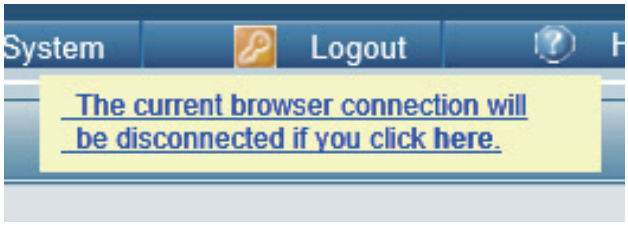
メモ

工場出荷時状態へのリセットは、本体のリセットボタンを押して行うこともできます。

Logout（ログアウト）

Web GUI画面からのログアウトを行います。

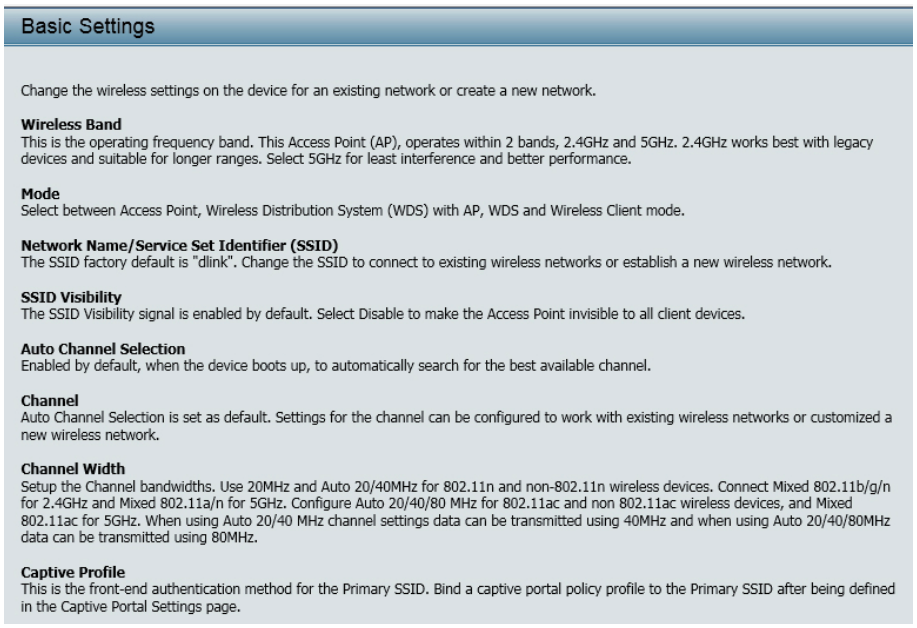
1. [Logout] アイコンをクリックします。
2. 以下のメッセージをクリックします。



Help（ヘルプ）

ヘルプ画面を表示します。

1. [Help] アイコンをクリックします。
2. 以下の画面でヘルプ情報を確認します。



付録

8

■ 工場出荷時設定に戻す 90
リセットボタンで設定リセット行う 90
Web GUIから設定リセットを行う 90
■ FAQ 91

工場出荷時設定に戻す

本製品の設定を工場出荷時の状態に戻す方法について説明します。

重要

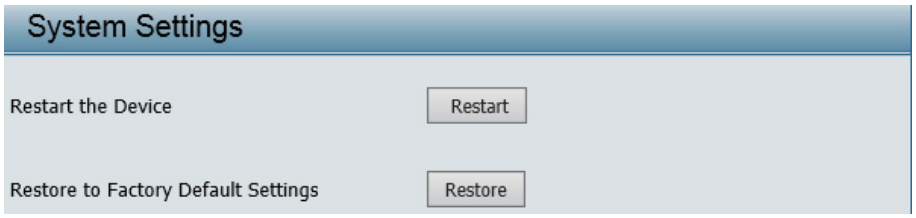
- 設定のリセットを行う前に、必要に応じて設定をバックアップしてください。
- リセット後のIPアドレスは「192.168.0.50」になります。

■リセットボタンで設定リセット行う

1. 本体の電源をいれた状態で、本体背面のリセットボタンを 10 秒以上押します。
2. ボタンを離すと、本体が再起動します。そのままお待ちください。

■Web GUIから設定リセットを行う

1. [System] アイコンをクリックします。
2. [Restore] をクリックします。



3. 以下の画面が表示され、再起動が行われます。

⚠注意

電源を切らずにそのままお待ちください。

FAQ

よくお問い合わせいただく内容について記載しています。

Q 本製品の設定を行うコンピュータからWeb ベースの設定メニューにアクセスできません。

A ①Webブラウザが本製品の対応しているバージョンであるか確認してください。

②本製品前面にあるLAN LED が点灯していることを確認してください。
LED が点灯していない場合は、UTP ケーブルが正しくポートに接続されているか確認してください。

③設定用PC のIP アドレスが本製品と同じアドレス範囲およびサブネット内であるか確認してください。

④コンピュータ上のすべてのインターネットセキュリティソフトウェアの動作を無効にしてください。
Zone Alarm、Black Ice、Sygate、Norton Personal ファイアウォール、およびWindows XP ファイアウォールなどのソフトウェアファイアウォールは設定ページへのアクセスを妨害する可能性があります。

⑤上記の点を確認してもアクセスできない場合は、一度本体の電源を抜き、約30秒後に再接続してみてください。

Q パスワードを忘れた場合はどうすればよいでしょうか。

A 設定のリセットを行ってください。→『工場出荷時設定に戻す：p.90 』

Q 無線接続が途切れます。対処方法を教えてください。

A ①アンテナの向きを変えてみてください。
またアンテナが壁や物から15cm以上離れるように本製品を設置してみてください。

②電波の干渉要因となるものから遠ざけてください。
2.4GHz 帯デジタルコードレス電話、X10 モジュールなどを使用したホームセキュリティシステム、天井設置型の扇風機、電灯、他の無線製品電波などとの干渉により、通信品質が激しく低下して通信ができなくなる場合があります。ご使用のルータ、アクセスポイントおよび無線LAN アダプタのチャンネルを変えて、干渉を回避してください。

③本製品は、電子レンジやモニタ、モータなどRF ノイズを発生する電気機器から90 ～ 180cm 以上離した場所に設置してください。